ALFAMA CURSOS

alfamacursos.com.br

Alfama Cursos

Antônio Garcez
Fábio Garcez
Diretores Geral

Antônio Álvaro de Carvalho
Diretor Acadêmico

MATERIAL DIDÁTICO

Produção Técnica e Acadêmica

Marcela Menezes Flores
Coordenadora Geral

Patrícia Queiroz de Meneses
Coordenadora Pedagógica

José Alves Correia Neto
Renata Jacomo Viana
Autoria

Gabriella Caroline Teles Silva
Sabina Regina Conceição Santos
Revisão Textual

Rafael Rezende de Farias
Editoração

Todos os direitos reservados e protegidos pela Lei 9.610 de 19/02/98.
É proibida a reprodução total ou parcial, por quaisquer meios, sem autorização prévia, por escrito, da ALFAMA CURSOS.

alfamacursos.com.br

Redes e Cabeamento

Apresentação do Curso

A conectividade é a palavra-chave do mundo globalizado e tecnológico em que vivemos, as redes de comunicação fazem parte do nosso dia a dia, seja no trabalho ou na vida pessoal, estamos sempre interligados. O mercado é competitivo e exige do profissional formação adequada e continuada. Esta disciplina mostrará a você caminhos para manter-se qualificado, podendo superar com empenho, as expectativas no mercado de trabalho.

Apresentação do Professor

JOSÉ ALVES NETO é graduado em Gestão de T.I. e pós-graduado em Gestão de Infraestrutura de Redes, pela Universidade Tiradentes (UNIT). Atua como analista de Tecnologia da Informação pela Prefeitura de Aracaju e como professor da Alfama Cursos. Está há mais de 5 anos na área de ensino de Informática, além de ser Certificado em Linux - LPIC - *Linux Professional Institute Certified.*

Componente Curricular

EMENTA

História, Informação e Comunicação; Utilização de Redes de Computadores; Modelos de Referência; Tipologia; Redes Wireless; Cliente – Servidor; Camadas de Transporte e Aplicação; Segurança de Redes; Firewall; Cabeamento Estruturado.

OBJETIVOS

Proporcionar ao educando a formação necessária na área de Infraestrutura de Redes e Cabeamento, aplicando conhecimento na utilização das redes de computadores, desenvolvendo habilidades e competências (cognitiva, produtiva, relacional) necessárias ao novo perfil profissional exigido pelo mercado.

HABILIDADES E COMPETÊNCIAS ESPERADAS

- Compreender a evolução histórica das redes de computadores.
- Conhecer os meios de comunicação e suas características.
- Conhecer os princípios de funcionamento das redes de computadores.
- Capacidade de entender a estrutura de cabeamento.
- Capacidade de conhecer adequadamente o funcionamento das redes e cabeamento estruturado.

PÚBLICO-ALVO

Candidatos que estejam cursando ou tenham concluído o ensino médio, ser maior de 18 anos.

Índice

Capítulo 1 - História – Como tudo começou 12
1.1 - Crescimento das Redes 14
1.2 – Exercício Proposto 15
Capítulo 2 – Informação e Comunicação 16
2.1 - Interação, Tecnologia de Telefonia e Informações 16
2.2 - Comunicação 16
2.2.1 - Comunicação em Rede 17
2.2.2 - Teleprocessamento 18
2.3 - TIC´s - Tecnologia da Informação e Comunicação 18
2.4 - Exercício Proposto 20
Capítulo 3 - Comunicação de Dados 21
3.1- Sinal Analógico 21
3.2 - Sinal Digital 21
3.3 - Comunicação de Dados Analógica e Digital 22
3.4 - Sistema De Transmissão 22
3.4.1 - Transmissão Analógica 22
3.4.2 - Transmissão Digital 23
3.5 - Vantagens Da Transmissão Digital 23
3.5.1 – Multiplexação 23
Capítulo 4 – A Utilização das Redes de Computadores 24
4.1 - Aplicações Comerciais 24
4.1.1 - Modelo Cliente-Servidor 25
4.2 - Aplicações Domésticas 25
4.3 - Usuários Móveis 26
4.4 - As Redes Sociais e os Problemas 27
4.5 – Exercício Proposto 28
Capítulo 5 – Modelos de Referência OSI e TCP/IP 29
5.1 - Modelo OSI 29
5.1.1 - Organização do Modelo OSI 30
5.2 - O Modelo OSI 30
5.3 - Modelo TCP/IP 30
5.3.1 - TCP/IP 31
5.3.2 - Aplicações TCP/IP 32
5.3.2.1 - SMTP 32
5.3.2.2 - FTP 32
5.3.2.3- Telnet 32
5.4 - Comparação entre os Modelos de Referência OSI e TCP/IP 32
5.5 - Termos de Interconexão de Redes 32
5.6 – Exercício Proposto 34
Capítulo 6 - Classificação e Topologia de Redes 35
6.1 - Redes Locais e Dispositivos 35
6.1.1 - LAN´s 36
6.1.1 - Dispositivos 36
6.2 - WAN (Wide Area Networks) 36
6.2.1 - Dispositivos 37
6.3 - Man (Metropolitan Area Network) 37
6.4 - Topologia de Redes 37
6.4.1 - Topologia Física 38
6.4.1.1 - Topologia de Barramento 38
6.4.1.2 - Topologia Anel 38
6.4.1.3 - Topologia Estrela 38
6.5 - Equipamentos de Interconexão 39
6.5.1 - Dispositivos de Redes 39
6.6 - Exercício Proposto 41
Capítulo 7 - Endereçamento da Internet 42

7.1 - Classes de Redes 42
7.2 - Sistema Binário 43
7.3 - IPv 44
7.4 - Endereços IP Privados 45
7.5 - IP Estático e IP Dinâmico 46
7.6 - Endereçamento 46
7.6.1 - Modos de Endereçamento 46
7.6.2 - Sentido de Transmissão ou Modo de Operação 46
7.6.2.1 - Simplex 46
7.6.2.2 - Half Duplex ou Semiduplex 46
7.6.2.3 - Duplex ou Full Duplex 47
7.6.3 - Controle de Erros 47
7.7 - Controle de Fluxo 47
7.8 - Exercício Proposto 48
Capítulo 8 – Redes Wireless 49
8.1 - Padrões 49
8.2 – Técnicas de Transmissão 50
8.3 – Elementos de Hardware 50
8.4 – Tipos de WLAN 51
8.4.1 - Indoor 51
8.4.2 - Outdoor 52
8.5 - Aplicações 52
8.5.1 - Expansão da Rede Cabeada 52
8.5.2 - Conexão entre Prédios 52
8.5.3 - Serviços de Última Milha 52
8.5.4 - Mobilidade 53
8.5.6 - Escritórios Móveis 53
8.5.7 - Hostspots 53
8.5.8 - Uso Doméstico 53
8.6 - Pontos de Acesso (AP) 53
8.6.1 – Modos de Operação 54
8.6.1.1 – Modo Root 54
8.6.1.2 – Modo Ponte 54
8.6.1.3 – Modo Repetidor 54
8.7 - Redes sem Fio (Wireless) 54
8.7.1 - Quais são os riscos do uso de Redes sem Fio? 55
8.7.2 - Que cuidados devo ter com um cliente de uma Rede sem Fio? ..... .55
8.7.3 - Que cuidados devo ter ao montar uma Rede sem Fio Doméstica? 56
8.7.4 - Explicação sobre SSID 56
8.8 - Exercício Proposto 57
Capítulo 9 – Computação Cliente – Servidor 58
9.1 - A Rede 58
9.2 – Evolução da Computação – Cliente-Servidor 58
9.3 - Aplicações Cliente-Servidor 59
9.4 - Terminologia de Cliente-Servidor 59
9.4.1 - Application Programming Interface (API) 59
9.4.2 - Cliente 59
9.4.3 - Middleware 59
9.4.4 - Bando de Dados Relacional 59
9.4.5 - Servidor 60
9.4.6 - Structured Query Language (SQL) 60
9.5 - Classes de Aplicações Cliente-Servidor 60
9.5.1 - Processamento baseado em Host 60
9.5.2 - Processamento baseado em Servidor 60
9.5.3 - Processamento baseado em Cliente 60
9.5.4 - Processamento Cooperativo 60
9.6 - Exercício Proposto 61
Capítulo 10 – Camada de Transporte 62

10.1 - Camada Física 62
10.2 - Camada Enlace de Dados 62
10.3 - Camada de Rede 62
10.4 - Camada de Transporte 62
10.4.1 - Serviços de Transporte 62
10.4.2 - Qualidade de Serviço 63
10.4.3 - As Primitivas da Camada de Transporte 63
10.4.4 - Elementos da Camadade Transporte 63
10.4.5 - Multiplexação 64
10.4.6 - Procolo Udp 64
10.5 – Exercício Proposto 65
Capítulo 11 – Camada de Aplicação 66
11.1 - DNS – Domain Name System – Sistema de Nomes de Domínios 66
11.2 - HTTP - O que é? 66
11.2.1 – Funcionamento 67
11.3 - FTP - O que é? 67
11.3.1 – Funcionamento 67
11.4 - SMTP - O que é? 68
11.4.1 - Funcionamento 68
11.5 - POP - O que é 68
11.5.1 – Funcionamento 68
11.6 – Exercício Proposto 70
Capítulo 12 - Segurança de Redes 71
12.1 – Segurança da Informação nas Redes 71
12.2 – Política de Segurança na Informação 72
12.3 – Incidentes de Segurança 72
12.4 - Técnicas de Segurança da Informação 73
12.5 – Requisitos de Segurança 74
12.5.1 - Privacidade 74
12.5.2 - Integridade 74
12.5.3 - Disponibilidade 74
12.5.4 - Autenticidade 74
12.6 - Execício Proposto 75
Capítulo 13 - Administração e Operação Segura de Redes e Sistemas 76
13.1 - Educação dos Usuários 76
13.2 - Ajuste do Relógio 76
13.2.1 - Sincronização de Relógios 76
13.2.2 - Timezone 77
13.3 - Equipes de Administradores 77
13.3.1 - Comunicação Eficiente 77
13.3.2 - Controle de Alterações da Configuração 77
13.3.3 - Uso de Contas Privilegiadas 78
13.4 - Logs 78
13.4.1 - Geração de Logs 78
13.4.2 - Armazenamento de Logs 78
13.5 - Cuidados com Redes Reservadas 79
13.6 – Exercício Proposto 81
Capítulo 14 – Firewall 82
14.1 - Finalidade do Firewall 82
14.2 - Tipos de Firewall 82
14.2.1 - Filtros Inteligentes 82
14.2.2 - Os Servidores Proxy 83
14.3 - Um exemplo de Firewall: IPTABLES 83
14.4 - Firewall é totalmente seguro? 83
14.5 - Exercício Proposto 119 85
Capítulo 15 - Conceito de Cabeamento - Normas de Cabeamento 86
15.1 - História 86
15.2 - Características do Cabeamento Estruturado 86

15.3 - Cabeamento Estruturado 87
15.4 - Normas Estruturais 88
15.5 - Principais Normas 88
15.6 - Exercício Proposto 89
Capítulo 16 – Elementos Ativos 90
16.1 - Ativos de Rede 90
16.2 - Repetidores 90
16.3 - Hub 90
16.4 - Bridges 91
16.5 - Switches 92
16.6 – Roteadores 92
16.6.1 - Serviços Oferecidos 92
16.6.2 - Componentes dos Roteadores 93
16.7 – Exercício Proposto 94
Capítulo 17 – Cabos e Conectores 95
17.1 - Tipos de Cabos 95
17.1.1 - Cabo Coaxial 95
17.1.1.1 - Meios de Transmissão 96
17.1.1.2 - Tipos de Cabos 96
17.1.2 - Cabo de Par Trançado 96
17.1.2.1 - Tipos de Cabos 97
17.2 - Definição das Categorias de Cabeamento 97
17.2.1 - Vantagens do Cabo UTP 98
17.3 - Fibra Óptica 98
17.3.1 – Sistema de Transmissão 99
17.3.2 - O Meio de Transmissão (Fibra) 99
17.4 - Princípio de Funcionamento 99
17.4.1 - Tipos de Fibras 99
17.5 - Conectores 100
17.6 – Instalação 100
17.7 - Rj-45 Fêmea (Jack) 101
17.7.1 – Instalação 101
17.8 - Imagens de Equipamentos para Cabeamento 102
17.9 – Exercício Proposto 105
Capítulo 18 – Projetando uma Estrutura e Utilização de Equipamentos para Infraestrutura de Cabeamento 106
18.1 - Levantamento das Necessidades 106
18.1.1 - Necessidades dos Futuros Usuários 106
18.2 - Levantamento por Área 106
18.3 - Componentes 107
18.4 - Patch Panel 107
18.5 – No-Breaks 107
18.6 – Importante! 108
18.7 - Exercício Proposto 109
Capítulo 19 - Projeto de Cabeamento Estruturado 110
19.1 - Objetivo 110
19.2 - Escopo 110
19.2.1 - Sumário do Projeto 110
19.3 - Tecnologias 110
19.3.1 - Rede Lógica 110
19.4 - Estações de Trabalho 110
19.4.1 - Térreo 110
19.4.2 – 1º Andar 111
19.5 - Sala de Equipamentos 111
19.6 - Cabeamento 111
19.7 - Junção 111
19.7.1 - Luvas 111
19.7.2 - Normas Utilizadas – Rede Lógica 112

19.8 - Lista de Materiais 112
19.9 - Equipamentos 112
19.10 - Outros Equipamentos 113
19.11 - Custo da Obra 113
19.12 - Custo Total 113
Respostas dos Exercícios Propostos 115
Referências 117
Referências das Figuras 118

1 - HISTÓRIA – COMO TUDO COMEÇOU

Cada um dos três séculos anteriores foi dominado por uma única tecnologia. O século XVIII foi a época dos grandes sistemas mecânicos que acompanharam a Revolução Industrial. O século XIX foi a era das máquinas a vapor. As principais conquistas tecnológicas do século XX se deram no campo da aquisição, do processamento e da distribuição de informações. Entre outros desenvolvimentos, vimos a instalação das redes de telefonia em escala mundial, a invenção do rádio e da televisão, o nascimento e o crescimento sem precedentes da indústria de informática e o lançamento dos satélites de comunicação.

Como resultado do rápido progresso tecnológico, essas áreas estão convergindo rapidamente e são cada vez menores as diferenças entre coleta, transporte, armazenamento e processamento de informações. Organizações com centenas de escritórios dispersos por uma extensa área geográfica podem com um simples apertar de um botão, examinar o status atual de suas filiais mais remotas. À medida que cresce nossa capacidade de colher, processar e distribuir informações torna-se ainda maior a demanda por formas de processamento de informações ainda mais sofisticadas. Apesar da indústria de informática ainda ser jovem em comparação a outros setores industriais (por exemplo, o de automóveis e o de transportes aéreos), foi simplesmente espetacular o progresso que os computadores conheceram em um curto período de tempo. Durante as duas primeiras décadas de sua existência, os sistemas computacionais eram altamente centralizados, em geral instalados em uma grande sala com paredes de vidro, através das quais os visitantes podiam contemplar embevecidos, aquela maravilha eletrônica. Uma empresa de médio porte ou uma universidade contava apenas com um ou dois computadores, enquanto as grandes instituições tinham, no máximo, algumas dezenas. Era pura ficção científica a ideia de que, em apenas 20 anos, haveria milhões de computadores igualmente avançados do tamanho de um selo postal.

A fusão dos computadores e das comunicações teve uma profunda influência na forma como os sistemas computacionais eram organizados. O conceito de "centro de computação" como uma sala com um grande computador ao qual, os usuários levam seu trabalho para processamento agora está completamente obsoleto. O velho modelo de um único computador atendendo a todas as necessidades computacionais da organização foi substituído pelas chamadas **redes** de **computadores**, nas quais os trabalhos são realizados por um grande número de computadores separados, mas interconectados.

Na década de 60 era a rede telefônica quem dominava o mundo inteiro, utilizando comutação[1] de circuitos para transmitir informação entre origem e destino. Com o crescimento tecnológico, houve a necessidade de interligar computadores que pudessem ser compartilhados em lugares geograficamente diferentes.

De 1969 a 1972 foi criada a ARPANET, o embrião da internet que conhecemos hoje. A rede entrou no ar em dezembro de 1969, inicialmente com apenas quatro nós, que respondiam pelos nomes SRI, UCLA, UCSB e UTAH e eram sediados, respectivamente, no *Stanford Research Institute*, na Universidade da Califórnia, na Universidade de Santa Bárbara e na Universidade de Utah, nos EUA. Eles eram interligados através de links de 50 kbps, criados

1 - O termo comutação surgiu com o desenvolvimento das Redes Públicas de Telefonia e significa alocação de recursos da rede (meios de transmissão, etc.) para a comunicação entre dois equipamentos conectados àquela rede. A comutação pode ser por circuitos, mensagens ou pacotes, recursos para transferência de informação que se caracteriza pela utilização permanente destes recursos durante toda a transmissão. É uma técnica apropriada para sistemas de comunicações que apresentam tráfego constante (por exemplo, a comunicação de voz), necessitando de uma conexão dedicada para a transferência de informações contínuas.

usando linhas telefônicas dedicadas, adaptadas para o uso como link de dados. Pode parecer pouco, mas 50 kbps em conexões de longa distância era uma velocidade impressionante para a época, principalmente se considerarmos que os modems domésticos da década de 1970 transmitiam a apenas 110 bps (bits por segundo), o que corresponde a apenas 825 caracteres de texto por minuto.

ARPANET é ideia da construção de uma rede de computadores que pudesse trocar informações. Ela surgiu no *Advanced Research Projects Agency*, Arpa do Departamento de Defesa dos EUA, quando em 1962, a agência contratou J.C.R. Licklider para liderar as suas pesquisas através do *Information Processing Techniques Office* - IPTO, da agência. Um dos sonhos de Licklider era uma rede de computadores que permitisse o trabalho cooperativo em grupos, mesmo que fossem integrados por pessoas geograficamente distantes, além de permitir o compartilhamento de recursos escassos, como, por exemplo, o supercomputador ILLIAC IV, em construção na Universidade de Illinois, com o patrocínio da própria ARPA. O projeto foi amadurecendo e adquiriu o momento quando a ARPA contratou Lawrence Roberts, do *Lincoln Lab* do MIT, em 1967, para tornar a ideia uma realidade. Nesta mesma época Licklider tendo saído da ARPA em 1964, assumiu a direção do Projeto MAC no MIT.

Esta rede inicial foi criada com propósitos de teste e com o desafio de interligar quatro computadores de arquiteturas diferentes, porém a rede cresceu rapidamente e em 1973 já interligava trinta instituições, incluindo universidades, instituições militares e empresas. Para garantir a operação da rede, cada nó era interligado a pelo menos dois outros (com exceção dos casos em que isso realmente não era possível), de forma que a rede pudesse continuar funcionando mesmo com a interrupção de várias das conexões.

Em 1974 surgiu o TCP/IP, que acabou se tornando o protocolo definitivo para uso na ARPANET e mais tarde na internet. Uma rede interligando diversas universidades permitiu o livre tráfego de informações, levando ao desenvolvimento de recursos que usamos até hoje, como o e-mail, o Telnet e o FTP, que permitiam aos usuários conectados trocar informações, acessar outros computadores remotamente e compartilhar arquivos. Na época, *mainframes* com um bom poder de processamento eram raros e incrivelmente caros, de forma que eles acabavam sendo compartilhados entre diversos pesquisadores e técnicos, que podiam estar situados em qualquer ponto da rede.

Um dos supercomputadores mais poderosos da época, acessado quase que unicamente via rede, era o Cray-1 (fabricado em 1976). Ele operava a 80 MHz, executando duas instruções por ciclo, e contava com 8 MB de memória, uma configuração que só seria alcançada pelos PCs domésticos quase duas décadas depois.

Imagem 01

1.1 - CRESCIMENTO DAS REDES

Na década de 70 haviam aproximadamente 200 máquinas conectadas à ARPANET. Ao final da década de 80, o número de máquinas ligadas à internet pública, uma confederação de redes muito parecidas com a internet de hoje. Grande parte desse crescimento foi por um grande número de esforços distintos para interligar universidades. A BITNET processava e-mail e fazia transferência de arquivos entre diversas universidades no nordeste dos E.U.A. A CSNET (*Computer Science Network* – rede de ciência de computadores) foi criada para interligar pesquisadores de universidades que não tinham acesso a ARPANET. Em 1986 foi criada a NSFNET para prover acesso aos centros de supercomputação patrocinados pela NSF. Também nesta época foi desenvolvido o DNS (*Domain Name System*), usado para conversão dos endereços em forma de letras e palavras, pois são de mais fácil memorização para nós, na forma de endereço IP de 32 bits, a linguagem dos computadores.

Com a enorme evolução do serviço em redes, tanto em empresas como em lares surgiram além das redes Ethernet, que são redes locais, redes Intranet que são redes locais ligadas a grande rede mundial, muito utilizada pelas empresas hoje para diversos fins, como comunicação com filiais, comunicação entre setores através de um sistema em rede e etc.

A grande rede formada por redes menores é hoje o componente mais importante na área da comunicação, a popular e grande rede global de computadores, a internet, ainda não parou de crescer e com certeza não parará, pois o número de usuários tanto para fins empresariais como pessoais aumenta a cada dia, pois, hoje o custo para aquisição, ou acesso a uma rede é menor e tende a ficarem cada vez mais barato, e ainda as maiores dificuldades seriam condições técnicas.

Não podendo esquecer que a grande rede ainda continua com os três protocolos TCP, IP e UDP criados no fim da década de 70, é claro que aperfeiçoados. As estatísticas apontam que hoje há no mundo em torno de mais de 900 milhões de usuários devido a grande utilidade no gerenciamento empresarial, nas políticas, nas residências, escolas, projetos de inclusão digital e, em fim, na sociedade em geral e, que o acesso hoje além do computador ocorre pelo celular, PDAs e outros.

A rede sempre irá mudar, devido a demandas do tempo e do mercado, pois o tempo passa e os recursos devem passar também, é claro que os recursos úteis sempre irão ficar. Se formos analisar blogs, vídeos, chats, MSN, pesquisas, sites de relacionamentos entre outros são a base da internet hoje.

1.2 – EXERCÍCIO PROPOSTO

1 - Qual a rede chamada de "Embrião da Internet"?

_____
_____
_____

2 – INFORMAÇÃO E COMUNICAÇÃO

A comunicação de informações juntamente com as redes de computadores tornaram-se imprescindíveis para as organizações pequenas e grandes se desenvolverem de forma equilibrada. Uma empresa que ignora o crescimento das tecnologias de informações e comunicação estará fadada ao atraso na corrida global. No núcleo da transformação está a informação.

Somos inquestionavelmente dependentes dos computadores e dos dispositivos e serviços de comunicação que os conectam. A quantidade de computadores e terminais em funcionamento no mundo hoje está na ordem de centenas de milhões. Isso constitui uma massa crítica: a necessidade esmagadora das organizações e seus trabalhadores agora é por conectividade, por integração, por facilidade de acesso à informação. A tecnologia da comunicação de informações é fundamental para o sucesso da empresa. A tecnologia que está possibilitando grande parte disso é a interligação de redes.

2.1 - INTERAÇÃO, TECNOLOGIA DE TELEFONIA E INFORMAÇÕES

Sobre este tópico (STALLINGS, p.5) descreve de forma bem interessante. A convergência que se refere à união das tecnologias de telefonia e informação anteriormente distintas. Podemos pensar nessa convergência em termos de um modelo de quatro camadas das comunicações na empresa:

I - Aplicações - estas são vistas pelos usuários finais de uma empresa. A convergência integra aplicações de comunicação, como chamada de voz (telefone), correio de voz, correio eletrônico e mensagens instantâneas, com aplicações corporativas. Com a convergência (interação), as aplicações fornecem recursos que incorporam voz, dados e vídeo de uma maneira transparente e com valor agregado (Ex: Mensagem Multimídia).

II - Serviços - nesse nível o gerente lida com a rede de informações em termos de serviços que ela fornece para suportar as aplicações. O gerente de rede precisa de serviços de projetos, manutenção e suporte relacionados ao emprego de facilidades baseadas em convergência.

III - Gerenciamento - os gerentes de rede se ligam com a rede da empresa como um sistema provedor de função. Esses serviços de gerenciamento podem incluir a preparação de um esquema de autenticação; gerenciamento de capacidade para vários usuários, grupos e aplicações.

IV - Infraestrutura - a infraestrutura consiste em enlaces de comunicação, LAN´s, WAN´s e conexões de internet disponíveis à empresa. Capacidade de transportar voz pode redes de dados, como a internet.

2.2 - COMUNICAÇÃO

A comunicação é uma das maiores necessidades humanas, o homem foi criado para comunicar-se. A comunicação humana é um processo que envolve a troca de informações, e utiliza os sistemas simbólicos como suporte para este fim. Estão envolvidos neste processo uma infinidade de maneiras de se comunicar: duas pessoas tendo uma conversa face a face, ou através de gestos com as mãos, mensagens enviadas utilizando a rede global de telecomunicações, a fala, a escrita que permitem interagir com as outras pessoas e efetuar algum tipo de troca informacional.

Para que se estabeleça a comunicação é essencial a atuação de 5 elementos básicos:

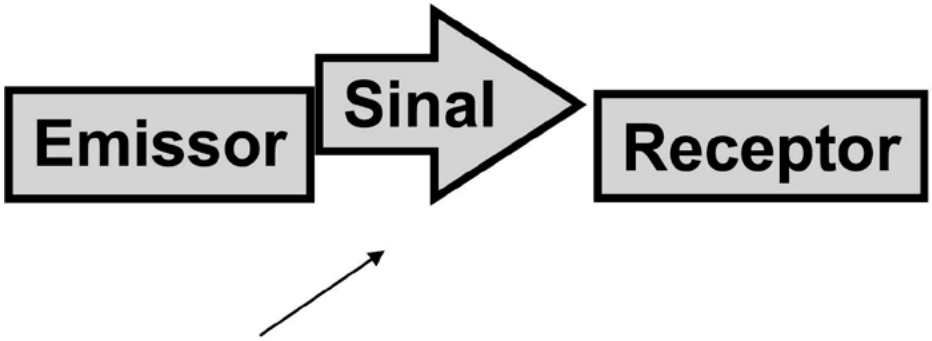
1. **O emissor:** responsável por transmitir a mensagem (informação).
2. **O receptor:** quem recebe a mensagem do emissor.
3. **O meio de transmissão:** interface ou caminho entre o emissor e receptor que transporta o sinal.
4. **O sinal:** um pacote que contém a mensagem composta de dados e informações.
5. **A linguagem:** norma ou padrão de comunicação estabelecido entre o emissor e o receptor.

O principal marco foi a invenção do telégrafo por Samuel Morse[2] em 1838. A partir daí a evolução dos sinais elétricos transmitidos a distância atravessou uma evolução muito grande. Por outro lado o armazenamento de dados e o tratamento de informações da década de 50 até os dias de hoje mudou a civilização ao ponto de caracterizá-la como a **ERA DA INFORMAÇÃO.**

Imagem 02

1838 – Samuel Morse realiza a primeira demonstração pública do telégrafo, em Nova Jersey.

Definimos comunicação como a transmissão de um sinal através de um meio, de um emissor para um receptor. O sinal contém uma mensagem composta de dados e informações. A informação é codificada em sinais apropriados que trafegam através de diferentes meios de transmissão. Observe a imagem abaixo:



Meio de transmissão

2.2.1 - COMUNICAÇÃO EM REDE

Comunicação em rede refere-se à transferência eletrônica de informações, comunicação mediada por um computador ou periférico. Com o surgimento das novas tecnologias como a internet tem facilitado à informação circular livremente, emitida de pontos diversos,

2 - Samuel Finley Breese Morse (1791 - 1872) foi um inventor, físico e pintor de retratos e cenas históricas estadunidenses. Tornou-se mundialmente célebre pelas suas invenções: o Código Morse e o telégrafo com fios, em 1843.

sendo encaminhada de maneira não linear a uma infinidade de outros pontos, que também são emissores de informação.

Dispositivos remotos de computador são capazes de se comunicar uns com os outros via sistemas de telecomunicações e de comunicação de dados. As telecomunicações se referem à transmissão eletrônica de sinais para comunicações, inclusive meios como telefone, rádio e televisão. As comunicações de dados, um subconjunto especializado de telecomunicações, se referem à coleta, processamento e distribuição eletrônica de dados entre dispositivos de hardware de sistemas de computador. As comunicações são obtidas através do uso da tecnologia de telecomunicações. Os meios de telecomunicações podem ser considerados qualquer coisa que carregue um sinal eletro/ eletrônico e faça uma intermediação entre um dispositivo que envia e um que recebe.

Um dispositivo de telecomunicações é um componente de hardware que permite que a comunicação de dados ocorra, ou que permite que a comunicação ocorra com mais eficiência.
As características de telecomunicações são:

- O tipo de sinal.
- A capacidade de transmissão.
- O modo de transmissão.

2.2.2 - TELEPROCESSAMENTO

O teleprocessamento é o processamento de dados executado remotamente com hardware e software voltados para comunicação e controlados por um conjunto de regras chamado de protocolos. O teleprocessamento utiliza recursos de telecomunicações. Surgiu devido à necessidade de se usar recursos entre sistemas diferentes e/ou distantes, provocando assim o surgimento das redes de computadores, como conhecemos hoje.

Telecomunicação + Processamento de dados vem revolucionando o mundo.

2.3 - TIC´S TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

A Tecnologia da Informação e Comunicação (TIC) pode ser definida como um conjunto de recursos tecnológicos, utilizados de forma integrada, com um objetivo comum. As TIC´s são utilizadas das mais diversas formas, na indústria (no processo de automação), no comércio (no gerenciamento, nas diversas formas de publicidade), no setor de investimentos (informação simultânea, comunicação imediata) e na educação (no processo de ensino aprendizagem, na Educação a Distância).

O desenvolvimento de hardwares e softwares garante a operacionalização da comunicação e dos processos decorrentes em meios virtuais. No entanto, foi a popularização da internet que potencializou o uso das TIC´s em diversos campos.

Através da internet, novos sistemas de comunicação e informação foram criados, formando uma verdadeira rede. Criações como o e-mail, o chat, os fóruns, a agenda de grupo on-line, comunidades virtuais, webcam, entre outros, revolucionaram os relacionamentos humanos.

Através do trabalho colaborativo, profissionais distantes geograficamente trabalham em equipe. O intercâmbio de informações gera novos conhecimentos e competências entre os profissionais.

Novas formas de integração das TIC´s são criadas. Uma das áreas mais favorecidas com as TIC´s é a educacional. Na educação presencial, as TIC´s são vistas como potencializadoras dos processos de ensino-aprendizagem. Além disso, a tecnologia traz a possibilidade de maior desenvolvimento – aprendizagem – comunicação entre as pessoas com necessidades

educacionais especiais.

As TIC´s representam ainda um avanço na Educação a Distância. Com a criação de ambientes virtuais de aprendizagem, os alunos têm a possibilidade de se relacionar, trocando informações e experiências. Os professores e/ou tutores tem a possibilidade de realizar trabalhos em grupos, debates, fóruns, dentre outras formas de tornar a aprendizagem mais significativa. Nesse sentido, a gestão do próprio conhecimento depende da infraestrutura e da vontade de cada indivíduo.

A democratização da informação, aliada a inclusão digital, pode se tornar um marco dessa civilização. Contudo, é necessário que se diferencie informação de conhecimento. Sem dúvida, vivemos na Era da Informação.

2.4 - EXERCÍCIO PROPOSTO

1 - Para que se estabeleça a comunicação é essencial a atuação de 5 elementos básicos. Quais são eles?

_____
_____
_____

3 - COMUNICAÇÃO DE DADOS[3]

As informações são transmitidas por meio de sinais eletromagnéticos, para que você possa entender um sinal eletromagnético é uma função de tempo ou função de frequência. Um sinal consiste em componentes de diferentes frequências. Dividimos um sinal eletromagnético como: analógico e digital.

3.1- SINAL ANALÓGICO

Sinal analógico é um tipo de sinal contínuo que varia em função do tempo. Um velocímetro analógico de ponteiros, um termômetro analógico de mercúrio, uma balança analógica de molas, são exemplos de sinais lidos de forma direta sem passar por qualquer decodificação complexa, pois as variáveis são observadas diretamente. Para entender o termo analógico, é útil contrastá-lo com o termo digital. "O sinal analógico é aquele que a intensidade do sinal varia de maneira uniforme com o tempo, não há pausas ou descontinuidade do sinal." O padrão analógico de transmissão de dados consiste na geração de sinais elétricos baseados nas ondas eletromagnéticas que são contínuas. Como os sinais analógicos são contínuos, a qualidade de operação é mais exigente, pois na sua falha, o sinal deve ser gerado novamente desde o princípio.

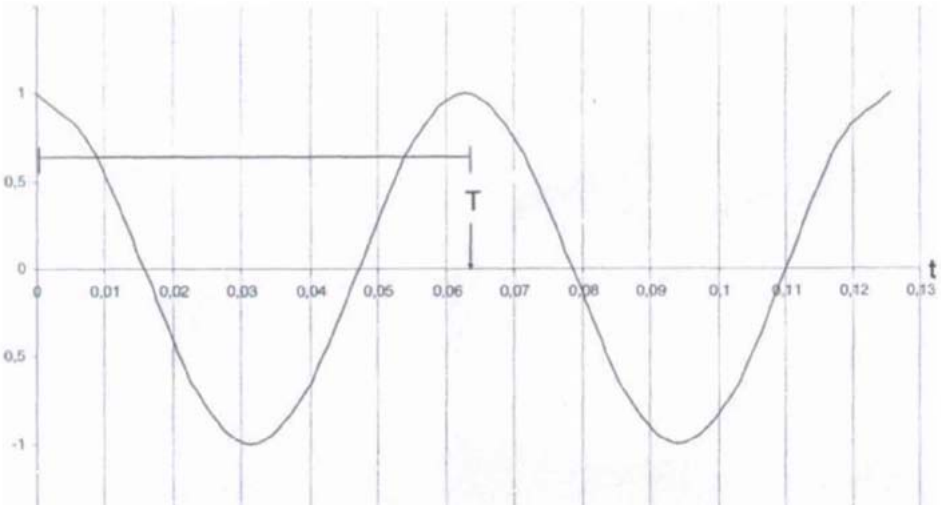


Imagem 04
Imagem de Sinal Analógico

3.2 - SINAL DIGITAL

Sinal digital é aquele que a intensidade do sinal se mantém num nível constante por algum tempo e, depois, muda para outro nível constante.

O sinal analógico poderia representar a fala, e o sinal digital poderia representar 1s e 0s binários. Chama-se binária porque é formada por dois dígitos apenas. Numa quantização de 8 bits, por exemplo, essa palavra poderia ter como valor 01001101, ou 11000101 ou qualquer combinação possível entre 00000000 e 11111111.

O padrão de comunicação digital consiste em pegar nos sinais analógicos, sejam de áudio ou vídeo e, parti-los em pequenos pedaços representados por um padrão binário, conhecido como zero e um. Cada pedaço deste sinal originalmente analógico vai ser identificado por este padrão digital e passará então a representar apenas aquele novo número binário,

3 - Capítulo retirado do livro de (STALLINGS) parte V – Comunicação de dados.

ou digital. Para entendermos melhor esta ideia, basta imaginarmos a palavra rádio. Se transmitida pelo sistema analógico, a sua modulação seria comprimida numa onda de rádio e transmitida por forma de ondas eletromagnéticas pelo espaço, mas pelo sistema digital, um conversor irá separar cada letra da palavra rádio e identificar este pedaço como uma sequência binária. Depois de transmitido, este sinal é recebido por um outro conversor que faz exatamente o contrário, recebe o sinal fracionado num conjunto de números e transforma-o em sinais eletromagnéticos analógicos. Este sistema de identificação analógica possui um padrão matemático. Cada conjunto de números 0 e 1 representa uma letra e porque este processo nunca se repete é que os conversores trabalham. Existem vários sistemas similares e compatíveis entre si para fazer estas conversões.

A principal vantagem entre os dois sistemas está no fato de que um sinal analógico quando é perdido, não pode ser reposto, porque ele é apenas uma onda de rádio, já um sinal digital, quando perdido ou corrompido (com defeito entre os dígitos) pode simplesmente ser repetido em tempo real, o que aumenta muito a dinâmica da transmissão.

3.3 - COMUNICAÇÃO DE DADOS ANALÓGICA E DIGITAL

Os sinais eletromagnéticos, capazes de se propagar por meio de uma variedade de meios de transmissão, podem ser usados para transportar dados. Os termos analógico e digital correspondem, grosseiramente, a contínuo e discreto, respectivamente. Estes dois termos costumam ser usados na comunicação de dados em pelo menos quatro contextos: dados, sinais, sinalização e transmissão. Para esclarecimento, definimos:

1. Dados como entidades que transportam informação.
2. Sinais são representações elétricas ou eletromagnéticas dos dados.
3. Sinalização é a propagação física do sinal ao longo de um meio adequado.
4. Transmissão é a comunicação dos dados pela propagação e pelo processamento dos sinais.

Os dados analógicos assumem valores contínuos em um intervalo, por exemplo, voz e vídeo, são padrões de intensidade continuamente variáveis. Os dados digitais assumem valores discretos; alguns exemplos são os textos e os dados binários. Em um sistema de comunicação, os dados são propagados de um ponto a outro por meio de sinais eletromagnéticos. Um sinal analógico e uma onda eletromagnética continuamente variável que pode ser transmitida por diversos meios, dependendo da frequência. Um sinal digital é uma sequência de pulsos de voltagem que pode ser transmitida sobre um meio fio, por exemplo. Uma voltagem positiva constante pode representar 0 binário, e um valor negativo constante pode representar 1 binário. Uma principal vantagem da sinalização digital é que geralmente é mais barata do que a sinalização analógica e é menos suscetível a interferências de ruído. Observe que a sinalização digital só é possível em meios de cobre, e não pode ser usada em fibra óptica ou meios sem fio. Tanto os dados digitais quanto os analógicos podem ser representados - e, portanto propagados - por sinais analógicos ou digitais.

3.4 - SISTEMA DE TRANSMISSÃO

O modo como os sistemas são tratados é uma função do sistema de transmissão.

3.4.1 - TRANSMISSÃO ANALÓGICA

É um meio de transmitir sinais analógicos independentemente do seu conteúdo; os sinais podem representar dados analógicos (voz) ou dados digitais (dados que passam por meio de um modem). Em qualquer caso, o sinal analógico sofrerá atenuação, o que limita a extensão do enlace de transmissão. Para obter distâncias mais longas, o sistema de transmissão analógica inclui amplificadores que aumentam a energia do sinal. Infelizmente o amplificador também aumenta os componentes do ruído. Com amplificadores instalados em cascata para obter longa distancia, o sinal se torna cada vez mais distorcido. Para

dados analógicos, como voz, bastante distorção pode ser tolerada sem que os dados se tornem ininteligíveis. Entretanto, para dados digitais transmitidos como sinais analógicos, os amplificadores em cascata aumentarão os erros.

3.4.2 - TRANSMISSÃO DIGITAL

A transmissão digital está voltada para o conteúdo do sinal. Sabemos que um sinal digital pode ser propagado apenas a uma distancia limitada antes da atenuação comprometer a integridade dos dados. Para conseguir distâncias maiores utilizam-se repetidores. Um repetidor recebe o sinal digital, recupera o padrão 1s e 0s e retransmite um novo sinal, sendo solucionada a atenuação. A mesma técnica pode ser utilizada com um sinal analógico, se for considerado que o sinal transporta dados digitais. Em pontos corretamente espaçados, sistema de transmissão possui dispositivos de retransmissão em vez de amplificadores. O dispositivo de retransmissão recupera os dados digitais do sinal analógico e gera um sinal digital novo e limpo. Portanto o ruído não é cumulativo.

3.5 - VANTAGENS DA TRANSMISSÃO DIGITAL

1. Custo - O surgimento da Large Scale Integration (LSI) e da Very Large Scale Integration (VLSI) causou uma contínua queda no custo e tamanho dos equipamentos digitais. Equipamentos analógicos não mostraram uma queda semelhante. Além disso, os custo de manutenção de sistemas são uma fração dos mesmos custos para os equipamentos analógicos.

2. Integridade de dados - Com o uso de repetidores digitais, em vez de amplificadores analógicos, os efeitos do ruído e outras deficiências de sinal não são cumulativos. Assim, é possível transmitir dados a distâncias maiores e por linhas de menor qualidade por meios digitais, sem comprometer a integridade dos dados.

3. Capacidade de utilização - Tornou-se econômico construir enlaces de transmissão com largura de banda extremamente alta, incluindo canais de satélite e fibra ótica. Um alto grau de multiplexação é necessário para utilizar eficazmente essa capacidade, e isso é obtido de modo mais fácil e barato com técnicas digitais (divisão de tempo) do que com técnicas analógicas (divisão de frequência).

4. Segurança e privacidade - Técnicas de criptografia podem ser facilmente aplicadas em dados digitais e em dados analógicos que foram digitalizados.

5. Integração - Tratando digitalmente as informações analógicas e digitais, todos os sinais tem a mesma forma e podem ser tratados de maneira semelhante, portanto, podem ser obtidas economias de escala e conveniência com a integração de voz, vídeo, imagem e dados digitais (STALLINGS, p.339).

3.5.1 – MULTIPLEXAÇÃO

A multiplexação consiste na operação de transmitir várias comunicações diferentes ao mesmo tempo através de um único canal físico. O dispositivo que afeta este tipo de operação chama-se multiplexador (multiplexer ou apenas mux). Apresentamos abaixo dois modos de efetuar a multiplexação:

a) Multiplexação por Divisão de Frequência (FDM - Frequency Division Multiplexing) - o espectro de frequências é dividido em diversas faixas, uma para cada transmissão ou comunicação distinta. Um exemplo é seu uso em sistemas de TV a cabo, que transportam múltiplos canais de vídeo em um único cabo.

b) Multiplexação por Divisão de Tempo (TDM - Time Division Multiplexing) - o tempo de transmissão de um canal é dividido em pequenas frações de tempo (iguais ou de acordo com uma proporção estatística), atribuindo-se uma fração a cada uma das várias transmissões que estão a decorrer ao mesmo tempo.

4 – A UTILIZAÇÃO DAS REDES DE COMPUTADORES

Antes de iniciarmos o exame detalhado das questões técnicas, vale a pena dedicar algum tempo a explicar por que as pessoas estão interessadas em redes de computadores e com que finalidade essas redes podem ser usadas. Afinal, se ninguém estivesse interessado em redes de computadores, poucas delas seriam elaboradas. Começaremos com os usos tradicionais em empresas e para indivíduos, e depois passaremos aos desenvolvimentos mais recentes relacionadas a usuários móveis e a redes domésticas.

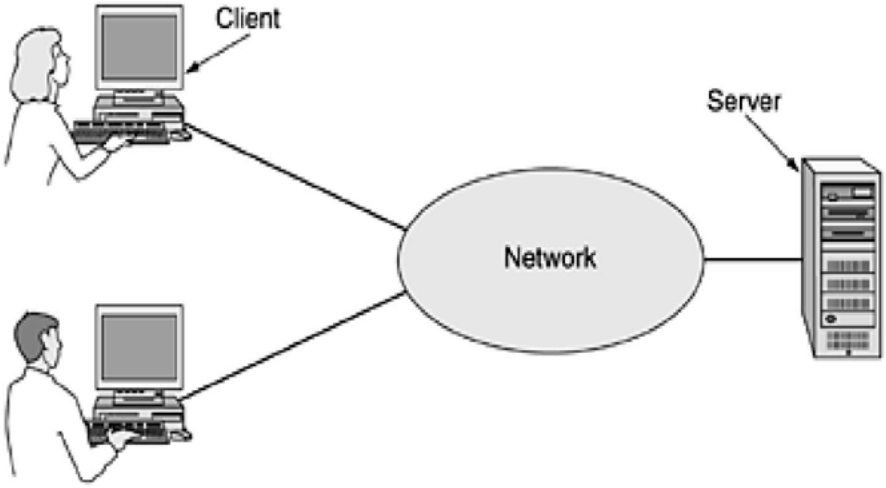
4.1 - APLICAÇÕES COMERCIAIS

Muitas empresas têm um número significativo de computadores. Por exemplo, uma empresa pode ter computadores separados para monitorar a produção, controlar os estoques e elaborar a folha de pagamento. Inicialmente, cada um desses computadores funcionava isolado dos outros, mas em um determinado momento, a gerência deve ter decidido conectá-los para poder extrair e correlacionar informações sobre a empresa inteira. Em termos um pouco mais genéricos, a questão aqui é o compartilhamento de recursos, e o objetivo é tornar todos os programas, equipamentos e especialmente dados ao alcance de todas as pessoas na rede, independente da localização física do recurso e do usuário. Um exemplo óbvio e bastante disseminado é um grupo de funcionários de um escritório que compartilham uma impressora comum. Nenhum dos indivíduos realmente necessita de uma impressora privativa, e uma impressora de grande capacidade conectada em rede muitas vezes é mais econômica, mais rápida e de mais fácil manutenção que um grande conjunto de impressoras individuais.

Porém, talvez mais importante que compartilhar recursos físicos como impressoras, scanners e gravadores de CD´s, seja compartilhar informações. Toda empresa de grande e médio porte e muitas empresas pequenas têm uma dependência vital de informações computadorizadas. A maioria das empresas tem registros de clientes, estoques, contas a receber, extratos financeiros, informações sobre impostos e muitas outras informações on-line. Se todos os computadores de um banco sofressem uma pane, ele provavelmente não duraria mais de cinco minutos. Uma instalação industrial moderna, com uma linha de montagem controlada por computadores, não duraria nem isso. Hoje, até mesmo uma pequena agência de viagens ou um a firma jurídica com três pessoas depende intensamente de redes de computadores para permitir aos seus funcionários acessarem informações e documentos relevantes de forma instantânea.

No caso de empresas menores, todos os computadores provavelmente se encontram em um único escritório ou talvez em um único edifício; porém, no caso de empresas maiores, os computadores e funcionários podem estar dispersos por dezenas de escritórios e fábricas em muitos países. Apesar disso, um vendedor em São Paulo às vezes poderia ter necessidade de acessar um banco de dados de estoque de produtos localizado nos Estados Unidos. Ou seja, a necessidade de utilizar dados, mesmo que eles estejam a quilômetros de distância.

No mais simples dos termos, é possível imaginar que o sistema de informações de uma empresa consiste em um ou mais bancos de dados e em algum número de funcionários que precisam acessá-los remotamente. Nesse modelo, os dados são armazenados em poderosos computadores chamados servidores. Com frequência, essas máquinas são instaladas e mantidas em um local central, por um administrador de sistemas. Em contraste, os funcionários têm em suas escrivaninhas máquinas simples (um PC comum), chamados clientes, com os quais eles acessam dados remotos, como por exemplo, para incluir em planilhas eletrônicas que estão elaborando. As máquinas clientes e servidores são conectados entre si por uma rede. Observe a figura abaixo.



4.1.1 - MODELO CLIENTE-SERVIDOR

Todo esse arranjo é chamado modelo cliente/servidor. Ele é amplamente utilizado e constitui a base da grande utilização da rede. Ele é aplicável quando o cliente e o servidor estão ambos no mesmo edifício (por exemplo, pertencem a mesma empresa), mas também quando estão muito distantes um do outro. Por exemplo, quando uma pessoa em sua casa acessa uma página na *World Wilde Web*, é empregado o mesmo modelo, com o servidor da Web remoto fazendo o papel do servidor e o computador pessoal do usuário sendo o cliente. Sob a maioria das condições, um único servidor pode cuidar de um grande numero de clientes.

4.2 - APLICAÇÕES DOMÉSTICAS

Em 1977, Ken Olsen era presidente da *Digital Equipment Corporation*, então o segundo maior fornecedor de computadores de todo o mundo (depois da IBM). Quando lhe perguntaram por que a Digital não estava seguindo a tendência do mercado de computadores pessoais, ele disse: *"Não há nenhuma razão para qualquer indivíduo ter um computador em casa".* A história mostrou o contrário, e a Digital não existe mais. Por que as pessoas compram computadores para usar em casa? No início, para processamento de textos e jogos; porém, nos últimos anos, esse quadro mudou exponencialmente. Cremos que agora a maior motivação seja o acesso à internet. Alguns dos usos mais populares da internet para usuários domésticos são:

1. Acesso a informações remotas.
2. Comunicação entre pessoas.
3. Entretenimento interativo.
4. Comércio eletrônico.

O acesso a informações remotas tem várias formas. Ele pode significar navegar nos sites Web para obter informações ou apenas por diversão, para estudo. As informações disponíveis incluem artes, negócios, culinária, governo, saúde, história, passatempos, recreação, ciência, esportes, viagens e muitos outros. A diversão surge sob tantas formas que não podemos mencionar, e também se apresenta em outras formas que é melhor não mencionarmos. Muitos jornais são publicados on-line e podem ser personalizados. Por exemplo, às vezes é possível solicitar todas as informações sobre políticos corruptos, grandes incêndios, escândalos envolvendo celebridades e epidemias, mas dispensar qualquer notícia sobre esportes. Algumas vezes, é até mesmo possível transferir os artigos selecionados por download para o disco rígido enquanto você dorme ou imprimi-los na sua impressora pouco antes do café da manhã. Além de jornais (e de revistas e periódicos científicos) temos também a biblioteca digital on-line. Muitas organizações profissionais,

como ACM (www.acm.org) e IEEE *Computer Society* (www.computer.org), já têm muitos periódicos e anais de conferências on-line. Observamos que quase tudo está sendo feito pela rede, (internet) conferências, estudo (EAD) compras, negócios, downloads dos mais diversos, (músicas, imagens, jogos, software, livros on-line).

Todas as aplicações anteriores envolvem interações entre uma pessoa e um banco de dados remoto repleto de informações. A segunda grande categoria de utilização de redes é a comunicação entre pessoas, basicamente a resposta do século XXI ao telefone do século XIX. O correio eletrônico (e-mail) já é usado diariamente por milhões de pessoas em todo o mundo e seu uso está crescendo rapidamente. Em geral, ele já contém áudio e vídeo, além de texto e imagens. Percebemos como a rede trouxe a facilidade na comunicação, vemos a junção de imagem, som, tecnologia, telefonia, sendo utilizadas na rede, em comunicação entre pessoas. Filhos quando viajam, falam com os pais pela webcam (com algum meio como MSN, Skype) reunião são feitas dessa forma, agilizando o processo de comunicação entre pessoas, grupos.

Hoje em dia, vemos a comunicação agilizada pela troca de mensagens instantâneas, não só para falar com amigo, mas muito utilizada nos negócio (esse recurso, derivado do programa Talk do UNIX, em uso desde aproximadamente 1970, permite que duas pessoas digitem mensagens uma para a outra em tempo real. Uma versão dessa ideia para várias pessoas é a sala de bate-papo (ou chat room), em que um grupo de pessoas pode digitar mensagens que serão vistas por todos.).

Newsgroups (grupos de notícias) mundiais, com discussões sobre todo tópico concebível, já são comuns entre grupos seletos de pessoas, e esse fenômeno crescerá até incluir a população em geral. O tom dessas discussões, em que uma pessoa divulga uma mensagem e todos os outros participantes do newsgroup podem ler a mensagem, poderá variar de bem-humorado a inflamado. Vemos o Orkut que ganhou espaço no Brasil que qualquer outro, depois o Facebook, gigante lá fora (América) crescente aqui no Brasil, e o Twitter, utilizado para comunicação rápida por meio de mensagens.

O que vemos hoje é que em qualquer lugar que você esteja, pode receber mensagens através dos dispositivos móveis, pode responder, acessar a conta do Facebook, e-mail ler as mensagens, respondê-las. Facilidade desse meio onde você utilizando celular, pode gravar uma cena que vê na rua, descaso, desrespeito às leis, e postá-las ficando disponível para todos os seus contatos. Transformou-se numa boa fonte de denúncia.

O entretenimento na rede está disponível também de forma aberta, descomplicada com recursos multimídias, transformou-se em uma nova maneira de diversão, não só para adolescentes, mas jovens e adultos. É visível o crescimento de crianças, adolescentes, jovens e adultos que utilizam a rede para se divertir, com jogos, músicas, enfim, diversas formas. E por fim, o comércio eletrônico que a cada ano cresce de forma extraordinária, chegando período de festas há um aumento significante em compras on- line, segundo dados de pesquisa do IPEA, cerca de 12 milhões de pessoas compras pela internet. Lembrando que devemos prestar atenção no quesito segurança, onde muitos compradores têm falhado.

4.3 - USUÁRIOS MÓVEIS

Computadores móveis, como notebooks e PDA´s (*Personal Digital Assistants*), constituem um dos segmentos de mais rápido crescimento da indústria de informática. Muitos usuários desses computadores têm máquinas de desktop no escritório e querem se manter conectados a essa base mesmo quando estão longe de casa ou em trânsito. Tendo em vista que é impossível ter uma conexão por fios em automóveis e aviões, existe um grande interesse em redes sem fios. As redes sem fios têm muitas utilidades. Um uso comum é o escritório portátil. Quando viajam, muitas vezes as pessoas querem usar seu equipamento eletrônico portátil para enviar e receber ligações telefônicas, fax e correio eletrônico, navegar pela Web, acessar arquivos remotos e se conectar a máquinas distantes. Além do mais, elas

querem fazer isso enquanto se encontram em qualquer lugar do planeta. Por exemplo, nas conferências de informática de hoje, os organizadores muitas vezes configuram uma rede sem fio na área de conferência. Qualquer pessoa com um notebook e um modem sem fio pode simplesmente ligar o computador e se conectar à internet, como se o computador estivesse ligado a uma rede de fiação. De modo semelhante, algumas universidades instalam redes sem fios no campus, para que os alunos possam se sentar debaixo das árvores e consultar o catálogo de fichas da biblioteca ou ler seu correio eletrônico.

As redes sem fios têm grande valor para frotas de caminhões, táxis, veículos de entrega e funcionários de serviços de assistência técnica, que precisam manter-se em contato com a base de operações da empresa.

4.4 - AS REDES SOCIAIS E OS PROBLEMAS

O crescimento das redes possibilitou também o movimento que chamamos de redes sociais, crescente hoje no mundo, onde as pessoas fazem um cadastro, escolhem um perfil que se adéque mais à sua necessidade e interesse, seja particular ou profissional. Muitas empresas de olho nessa crescente estatística passaram a utilizar as redes sociais em beneficio próprio, na contratação de pessoas, ou para compreender as necessidades dos clientes (através do perfil) e atendê-lo. O grande problema que destacamos é a falta de atenção ou de conhecimento por parte do usuário, em deixar muitas vezes sua imagem (e de sua família) exporta, permitindo assim que "ladrões virtuais" de forma fácil, roubem dados, comprometendo a vida. Insistimos em afirmar que as redes sociais são excelentes, porém, os cuidados com segurança de senhas devem ser levados em consideração. Não façamos como o velho ditado, depois que a casa é roubada é que se colocam fechaduras – algo mais ou menos assim.

4.5 – EXERCÍCIO PROPOSTO

1 - Como definimos dados?

_____
_____
_____

5 – MODELOS DE REFERÊNCIA OSI E TCP/IP

Vamos examinar neste capítulo modelos de referência da arquitetura de redes, modelo OSI e TCP/IP. Os modelos relacionados ao protocolo OSI raramente são utilizados hoje em dia, é importante entender esta arquitetura e suas camadas. O modelo TCP/IP tem características opostas ao modelo OSI.

5.1 - MODELO OSI

O modelo OSI foi desenvolvido pela ISO (International Standards Organization) como primeiro passo à padronização internacional dos protocolos empregados nas diversas camadas surgiu em 1984. O modelo é chamado: Modelo de Referência OSI (Open Systems Interconnection), pois ele trata de interconexão de sistemas abertos, isto é, sistemas que estão abertos à comunicação com outros sistemas. O modelo OSI tem sete camadas. São elas:

1. Física.
2. Enlace de dados.
3. Rede.
4. Transporte.
5. Sessão.
6. Apresentação.
7. Aplicação.

A tarefa da ISO foi definir um conjunto de camadas e os serviços realizados por camada. Cada camada fornece um conjunto de funções a camada superior, baseando-se nas funções que lhe são fornecidas pela camada inferior.

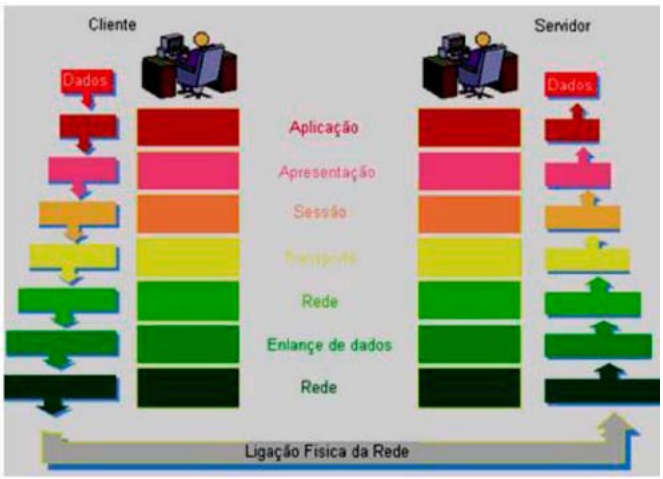


Imagem 5

A comunicação entre dois computadores A e B na figura acima. Se a aplicação A quiser enviar uma mensagem para aplicação B, ela invocará a camada de aplicação (camada 7). Esta camada estabelece uma relação de parceria com a camada 7 do computador de destino, usando o protocolo da camada 7 (protocolo de aplicação). Esse protocolo exige os serviços da camada 6, de modo que as duas entidades da camada 6 utilizam um protocolo próprio, e assim por diante até a camada física, que realmente transmite os bits por um meio de transmissão. Observe que não existe uma comunicação direta entre as camadas parceiras, exceto a camada física, então, acima da camada física, cada entidade de protocolo envia dados para a próxima camada inferior para levar os dados à sua camada parceira.

5.1.1 - ORGANIZAÇÃO DO MODELO OSI

1 - Camadas orientadas à Aplicação

- Sessão, Apresentação e Aplicação:

Estão relacionadas com o S.O. e o computador.

2 - Camada de Interface

- Transporte:

Fornece uma interface independente da rede para ser usado pelas camadas orientadas à aplicação.

3 - Camadas dependentes da Rede

- Física, ligação de dados e rede:

Dependem do meio físico de transmissão e da topologia de rede.

5.2 - O MODELO OSI

O modelo OSI tem três conceitos fundamentais:

1. Serviços.
2. Interfaces.
3. Protocolos.

Provavelmente, a maior contribuição do modelo OSI seja tornar explícita a distinção entre esses três conceitos. Cada camada executa alguns serviços para a camada acima dela. A definição do serviço informa o que a camada faz, e não a forma como as entidades acima dela o acessam ou como a camada funciona. Essa definição estabelece a semântica da camada.

A interface de uma camada informa como os processos acima dela podem acessá-la. A interface especifica quais são os parâmetros e os resultados a serem esperados. Ela também não revela o funcionamento interno da camada.

Finalmente, os protocolos utilizados em uma camada são de responsabilidade dessa camada. A camada pode usar os protocolos que quiser desde que eles viabilizem a realização do trabalho (ou seja, forneçam os serviços oferecidos). Ela também pode alterar esses protocolos sem influenciar o software das camadas superiores.

5.3 - MODELO TCP/IP

Vamos iniciar esse assunto sobre o modelo de referência TCP/IP com a ARPANET. A ARPANET era uma rede de pesquisa patrocinada pelo Departamento de Defesa dos Estados Unidos (DoD). Pouco a pouco, centenas de universidades e repartições públicas foram conectadas, usando linhas telefônicas dedicadas. Quando foram criadas as redes de rádio e satélite, começaram a surgir problemas com os protocolos existentes, o que forçou a criação de uma nova arquitetura de referência. Desse modo, a habilidade para conectar várias redes de maneira uniforme foi um dos principais objetivos do projeto, desde o início. Mais tarde, essa arquitetura ficou conhecida como modelo de referência TCP/IP, graças a seus dois principais protocolos. Esse modelo foi definido pela primeira vez em (Cerf e Kahn, 1974). Uma nova perspectiva foi oferecida mais tarde em (Leiner et al., 1985).

Diante da preocupação do Departamento de Defesa dos EUA de que seus preciosos hosts,

roteadores e gateways de interconexão de redes fossem destruídos de uma hora para outra, definiu-se também que a rede deveria ser capaz de sobreviver à perda do hardware de sub-redes, com as conversações existentes sendo mantidas em atividade. Em outras palavras, o Departamento de Defesa dos EUA queria que as conexões permanecessem intactas enquanto as máquinas de origem e de destino estivessem funcionando, mesmo que algumas máquinas ou linhas de transmissão intermediárias deixassem de operar repentinamente. Além disso, era necessária uma arquitetura flexível, capaz de se adaptar a aplicações com requisitos divergentes como, por exemplo, a transferência de arquivos e a transmissão de dados de voz em tempo real.

5.3.1 - TCP/IP

O TCP/IP (*Transmission Control Protocol/Internet Protocol*) é um padrão baseado na internet, sendo a estrutura para uma gama completa de padrões de comunicação por computador. Cremos que praticamente todos os fabricantes de computador oferecem suporte a esta arquitetura. O modelo TCP/IP foi desenhado para permitir interligação de redes distintas (heterogêneas) fisicamente. Um projeto destinado a interligar os computadores do governo americano que possuíam diferentes hardwares e sistemas.

No protocolo de comunicação estão definidas todas as regras necessárias para que o computador de destino, "entenda" as informações no formato que foram enviadas pelo computador de origem.

Antes da popularização da internet existiam diferentes protocolos sendo utilizados nas redes das empresas. Os mais utilizados eram os seguintes:

- TCP/IP.
- NETBEUI.
- IPX/SPX.
- Apple Talk.

O TCP/IP é dividido em cinco camadas e, em cada camada existem diferentes protocolos exercendo diversas funções. Como no início o modelo de referência OSI de 7 camadas ainda não tinha sido criado pela ISO (International Standarts Organization). Foi adotado o modelo de 5 camadas conhecido também pelo modelo DARPA.

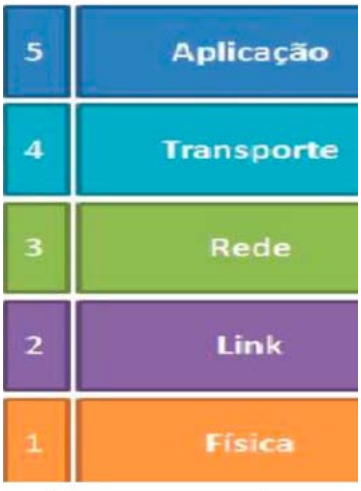


Imagem 6

Para entendermos melhor esta arquitetura é interessante conhecermos o conceito de protocolos.

Um protocolo é usado para comunicação entre entidades em diferentes sistemas, podemos exemplificar entidades como: programas de aplicação do usuário, pacotes de transferência

de arquivos, sistemas de gerenciamento de banco de dados, correio eletrônico, sobre sistemas podemos citar: computadores, terminais. De fora geral a entidade é algo que é capaz de enviar e receber informações, e o sistema é o objeto fisicamente distinto, que contém uma ou mais entidades. Para que as entidades se comuniquem de forma a se entenderem devem "falar a mesma linguagem". Definimos essa linguagem como protocolo, que definimos como um conjunto de regras controlando a troca de dados entre duas facilidades. Os principais elementos de um protocolo são:

- **Sintaxe** - inclui elementos como formato de dados e níveis de sinal.
- **Semântica** - inclui informações de controle para ordenação e tratamento de erro.
- **Temporização** - inclui combinação de velocidade e sequência.

5.3.2 - APLICAÇÕES TCP/IP

Entre as aplicações padronizadas para operar com TCP, mencionamos três: SMTP, FTP e TELNET.

5.3.2.1 - SMTP

O SMTP (*Simple Mail Transfer Protocol*) oferece a facilidade básica de correio eletrônico. Ele fornece um mecanismo de transferência de mensagens entres hosts separados. Recursos que o SMTP dispõe: lista de correspondência, recibos de retorno e encaminhamento. O protocolo SMTP não especifica o modo como as mensagens devem ser criadas; alguma facilidade local de edição ou correio eletrônico é necessária. Quando uma mensagem é criada, o SMTP aceita a mensagem e utiliza o TCP para enviá-la a um módulo SMTP ou outro host.

5.3.2.2 - FTP

O FTP (*File Transfer Protocol*) é usado para enviar arquivos via sistema para outro sob o comando do usuário. Arquivos de texto e binários são acomodados, e o protocolo oferece recursos para controlar o acesso do usuário. Ex. Transferência de arquivo para um provedor de internet.

5.3.2.3- TELNET

O TELNET oferece uma capacidade de logon remoto, que permite que um usuário em um terminal ou computador pessoal efetue logon com o computador remoto e utilize como se estivesse conectado a esse computador.

5.4 - COMPARAÇÃO ENTRE OS MODELOS DE REFERÊNCIA OSI E TCP/IP

Os modelos de referência OSI e TCP/IP têm muito em comum. Os dois se baseiam no conceito de uma pilha de protocolos independentes. Além disso, as camadas têm praticamente as mesmas funções. Por exemplo, em ambos os modelos estão presentes as camadas que englobam até a camada de transporte para oferecer um serviço de transporte fim a fim independente da rede a processos que desejam se comunicar. Essas camadas formam o provedor de transporte. Mais uma vez, em ambos os modelos, as camadas acima da camada de transporte dizem respeito aos usuários orientados a aplicações do serviço de transporte. Apesar dessas semelhanças fundamentais, os dois modelos também têm muitas diferenças.

5.5 - TERMOS DE INTERCONEXÃO DE REDES

STALLINGS, p. 139 descreve em seu livro Redes e Sistemas de Comunicação de Dados tais termos, como segue:

1. **Rede de comunicação:** Uma facilidade que oferece um serviço de transferência de dados entre dispositivos conectados à rede.

2. **Inter-rede:** Uma coleção de redes de comunicação interconectadas por pontes ou roteadores.

3. **Intranet:** Uma inter-rede usada por uma única organização, que oferece as principais aplicações de internet, especialmente a Word Wide Web (WWW). Uma intranet opera dentro da organização para fins internos e pode existir com uma inter-rede isolada, autocontida, ou pode ter links para a internet.

4. **Extranet:** A extensão da internet de uma empresa para a internet, permitindo que clientes, fornecedores e trabalhadores móveis selecionados acessem os dados e as aplicações privadas da empresa por meio da Word Wide Web.

5. **Sub-rede**: Refere-se a uma rede constituinte de uma inter-rede. Isso evita ambiguidade porque a inter-rede inteira, do ponto de visa de um usuário, é uma única rede.

6. **End System (ES)**: Sistema final. Um sistema conectado a uma das redes de uma inter-rede, que é usado para dar suporte a aplicações ou serviços do usuário final.

7. I**ntermediate System (IS)**: Sistema intermediário. Um dispositivo usado para conectar duas redes e permitir a comunicação entre os sistemas finais conectados a diferentes redes.

8. **Ponte**: Um IS usado para conectar duas LAN´s que utilizam protocolos de LAN semelhantes. A ponte atua como um filtro de endereços, selecionando pacotes de uma LAN que deverão seguir para um destino em outra LAN e passando esses pacotes adiante. A ponte não modifica o conteúdo dos pacotes e não acrescenta algo ao pacote. A ponte opera na camada 2 do modelo OSI.

9. **Roteador**: Um IS usado para conectar duas redes, que podem ser ou não semelhantes. O roteador emprega um protocolo de inter-rede presente em cada roteador e cada sistema final de rede. O roteador opera na camada 3 do modelo OSI.

5.6 – EXERCÍCIO PROPOSTO

1 - Quais as camadas do modelo de referência OSI?

_____
_____
_____

6 - CLASSIFICAÇÃO E TOPOLOGIA DE REDES

As redes de computadores estão cada vez mais presentes no dia a dia das pessoas, que estão conhecendo e adotando a interligação dos seus equipamentos como uma medida econômica e necessária para o bom funcionamento da empresa. Elas estão divididas em três categorias conforme sua abrangência geográfica:

a) **Rede local (LAN - Local Area Network)** - tem o objetivo de interligar computadores localizados na mesma sala, edifício ou campus, possuindo uma distância máxima de alguns quilômetros entre as estações mais distantes. Normalmente as redes locais possuem uma taxa de transferência de dados maior do que 1 Mbps e são propriedade de uma única organização.

b) Rede metropolitana (MAN - Metropolitan Area Network) - tem o objetivo de interligar computadores dentro da mesma cidade e arredores, possuindo distâncias até aproximadamente 100 km.

c) Rede de longa distância (WAN - Wide Area Network) - tem o objetivo de interligar computadores distantes um do outro, ou seja, computadores localizados em cidades, estados ou mesmo países diferentes. Normalmente as redes de longa distância são oferecidas por empresas de telefonia, não possuindo uma faixa de velocidades específica, pois basta o cliente ter necessidade e dinheiro que lhe será destinada uma largura de banda adequada. As velocidades variam bastante, indo desde 1200 Bps até 2,4 Gbps, logo chegando a 10 Gbps.

A figura abaixo nos traz visualmente o conceito.

Distância entre as CPUs	Localização das CPUs	Nome
0,1 m	Placa de circuito impresso Assist. dados pessoal	Placa-mãe Personal Area Network (PAN)
1,0 m	Milímetro Mainframe	Rede de sistemas de computadores
10 m	Sala	Redes locais (LANs) Sua sala
100 m	Prédio	Redes locais (LANs) Sua escola
1000 m = 1 km	Campus	Redes locais (LANs) Stanford University
100,000 m = 100 km	País	Rede de longa distância (WAN) Cisco Systems, Inc.
1.000.000 m = 1.000 km	Continente	Rede de longa distância (WAN) África
10.000.000 m = 10.000 km	Planeta	Rede de longa distância (WAN) A Internet
100.000.000 m = 100.000 km	Sistema Terra-Lua	Rede de longa distância (WAN) Terra e satélites artificiais

Imagem 7

6.1 - REDES LOCAIS E DISPOSITIVOS

6.1.1 - LAN´S

As LAN´s são usadas para interligar servidores, estações de trabalho, impressoras e outros equipamentos que possam ser compartilhados. As redes locais podem ser vistas hoje nos lares, ambientes comerciais, escolas, hospitais e edifícios próximos.

As LAN´s se destinam a:

- Operar dentro de uma área geográfica limitada.
- Permitir multiacesso a meios com muita largura de banda.
- Controlar de forma privada redes sob administração local.
- Fornecer conectividade em tempo integral com os serviços locais.
- Conectar fisicamente dispositivos adjacentes.

6.1.1 - DISPOSITIVOS

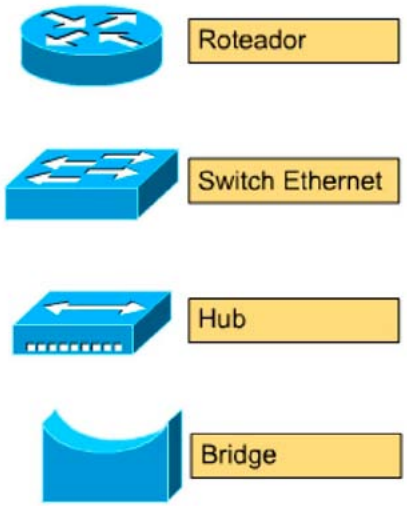


Imagem 8

6.2 - WAN (WIDE AREA NETWORKS)

Rede geograficamente distribuída é também conhecida como Rede de Longa Distância. Abrangendo uma grande área geográfica, teve seu início em 1965 quando Lawrence Roberts e Thomas Merril ligaram dois computadores de modelos diferentes, por meio de uma linha telefônica, o que depois vem a ser a internet.

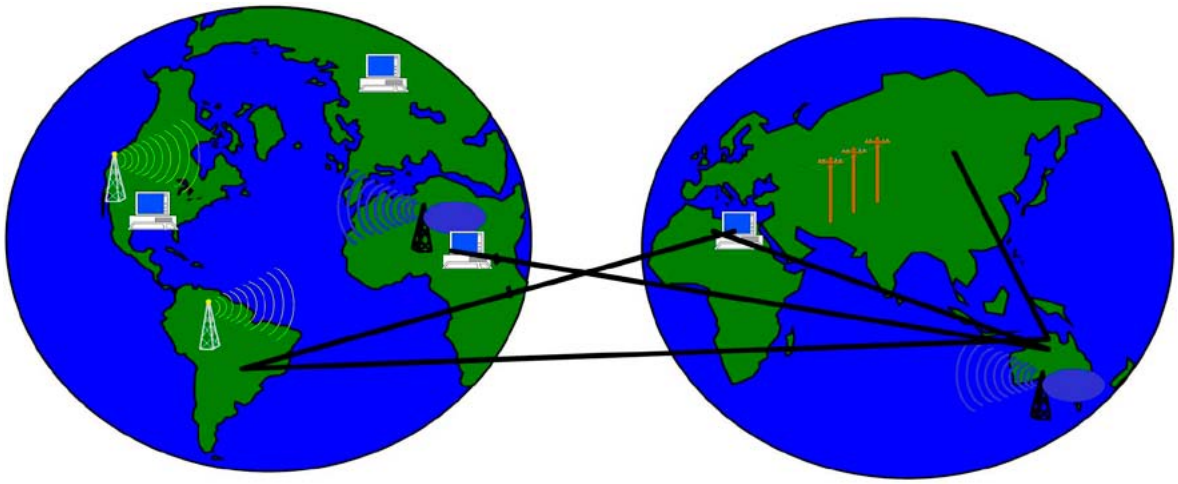


Imagem 9 e 10

As WAN´s se destinam a:

- Operar dentro de uma grande área geográfica.
- Permitir acesso a interfaces seriais em baixa velocidade.
- Fornecer conectividade em tempo integral e tempo parcial.
- Conectar dispositivos separados por amplas áreas geográficas.

6.2.1 - DISPOSITIVOS

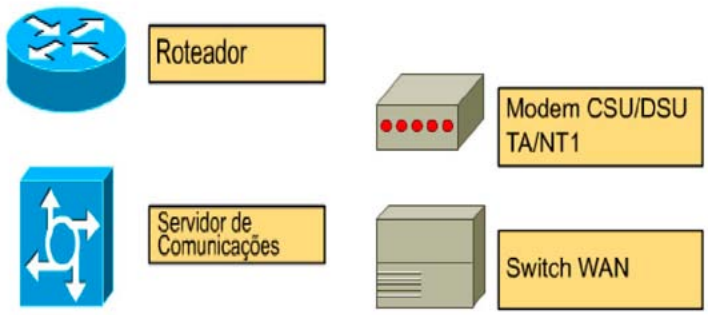


Imagem 11

6.3 - MAN – METROPOLITAN AREA NETWORK

A Rede Metropolitana apresenta as mesmas características da Rede Local, diferenciando quanto à cobertura de área e velocidade de transmissão. Devem ser aplicadas quando os módulos processadores (computadores de grande porte, microcomputadores) ultrapassam a distância de 25 km. Os sistemas de TV por assinatura (cabo e rádio) são hoje um exemplo prático dessa rede.

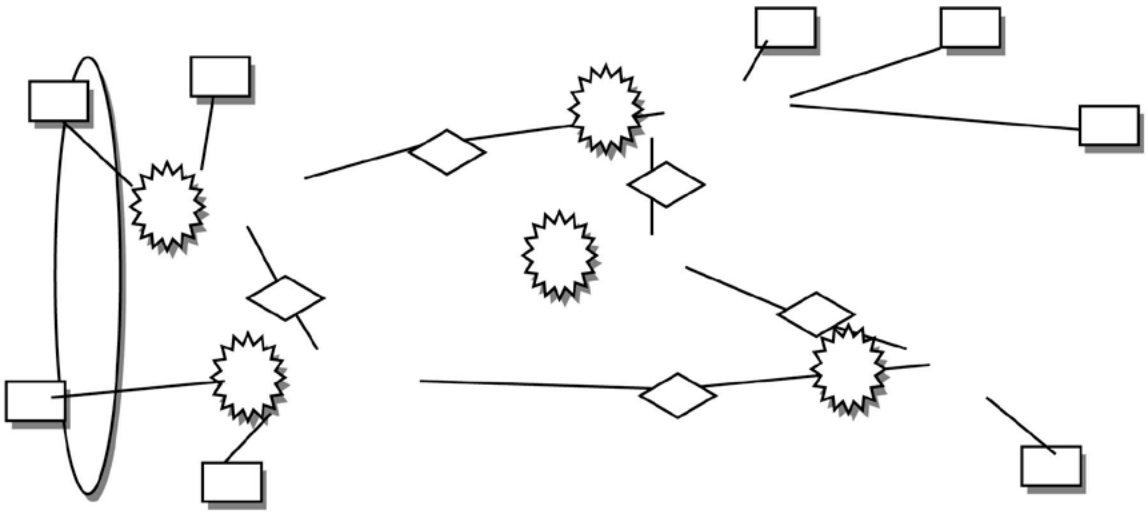


Imagem 12

- Redes Metropolitanas.
- Operam em áreas maiores que as LAN e com menores velocidades.
- O termo surgiu com o padrão IEE 802.6.

6.4 - TOPOLOGIA DE REDES

A topologia da rede define a estrutura da rede, ela é um diagrama que descreve como seus elementos estão conectados. Esses elementos são chamados de NÓS, e podem ser

computadores, impressoras e outros equipamentos. Existem duas partes na definição da topologia: a topologia física, que é o layout atual do fio (meio) e a topologia lógica, que define como os meios são acessados pelos hosts. As topologias físicas que são comumente usadas são: barramento, anel, estrela, estrela estendida, hierárquica e rede.

6.4.1 - TOPOLOGIA FÍSICA

Vamos conhecer três tipologias de rede: topologia de barramento, topologia anel e topologia estrela.

6.4.1.1 - TOPOLOGIA DE BARRAMENTO

Ligada por um conduto central, a rede em barra (também conhecida como rede em bus) utiliza o método de transmissão em paralelo, onde a mensagem é enviada por somente uma estação e as outras se encarregam de receber a mensagem. Caso mais de uma estação tente enviar uma mensagem ao mesmo tempo, poderá ocorrer um problema de fluxo de dados, comumente conhecido como colisão, causando atraso na rede, pois a mensagem será perdida e terá que ser reenviada ao meio.

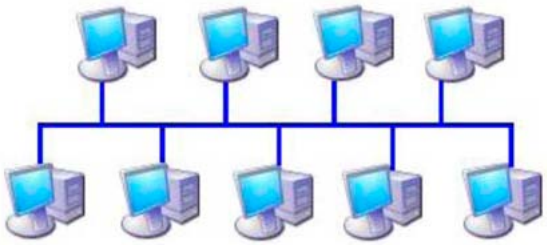


Imagem 13

6.4.1.2 - TOPOLOGIA ANEL

Uma topologia de rede anel apresenta-se hoje em poucas redes no mundo. Constituída pela distribuição de computadores em um circuito fechado, realiza sua comunicação em série, ou seja, o sinal transmitido passa por todas as estações necessárias até chegar ao seu destino. Usa o sentido bidirecional (o sinal trafega nos dois sentidos), sendo o método unidirecional mais utilizado para evitar colisão. Uma grande característica dessa rede é que os computadores não são diretamente ligados ao meio físico, e sim, por intermédio de equipamentos repetidores do sinal.

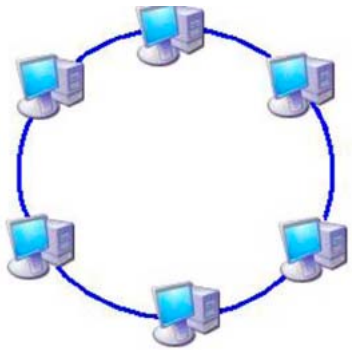


Imagem 14

6.4.1.3 - TOPOLOGIA ESTRELA

Também conhecida como rede estrela, necessita de um equipamento inteligente, concentrador de linhas (switches) para centralizar o tráfego dos dados na rede, enviando o dado apenas à estação destinatário, evitando que a mensagem seja enviada para todas as estações na rede. O mesmo não acontece com os hubs, que enviam as mensagens para todos os nós na rede. Essa é a grande diferença em pensar na topologia física da

mesma forma que se pensa nela logicamente. O fato é que, internamente, o hub possui um filamento ligado às entradas dos conectores que na verdade é uma barra, assunto que trataremos no próximo tópico.

Imagem 15

6.5 - EQUIPAMENTOS DE INTERCONEXÃO

Veremos com mais detalhes esses equipamentos quando tratarmos de cabeamento estruturado, porém, segue abaixo para conhecimento, alguns equipamentos necessários às redes.

- Os mais comuns são:

- Hub.
- Switches.
- Roteador.

- Outros: repetidor, ponte, gateway e etc.
- Gateway: conversor - adaptador de protocolos, velocidades, interfaces e etc.

6.5.1 - DISPOSITIVOS DE REDES

a) Placa de rede

As placas de rede são consideradas dispositivos da camada 2 (enlace) porque cada placa de rede em todo o mundo transporta um código exclusivo, chamado de Media Access Control (MAC). Esse endereço é usado para controlar as comunicações de dados do host na rede. Como o nome sugere, a placa de rede controla o acesso do host ao meio.

Imagem 16

b) Hub

Dispositivo utilizado para conectar os equipamentos de uma rede local. Hub ou concentrador (Stand Alone, Stackable, Modular/Chassi - eth/fddi/coax – ativo, passivo e inteligente).

Imagem 17

c) Switches

Os switches operam na camada 2 (enlace) encaminhando quadros ethernet pelo endereço MAC. Os switches operam ao nível de endereço MAC com as bridges (pontes), mas diferentemente delas, o switche é capaz de suportar muitas conexões, segmentando a rede de forma simples e eficaz. Uma diferença entre hub´s e switches: hubs encaminham os dados recebidos para todos equipamentos conectados à rede; switches encaminham os dados somente para a porta no qual está conectado o equipamento destino.

Imagem 18

d) Roteador

Dispositivo que decide qual o caminho o tráfego de informações deve seguir, baseado em endereços lógicos. Conectam LAN´s remotas ou a internet. O roteador opera na camada 3 (rede).

Imagem 19

e) Bridges (PONTES)

Bridges ou pontes são equipamentos que possuem capacidade de segmentar uma rede local em varias sub-redes, e com isso diminuir o fluxo de dados. Desta forma quando uma estação envia um sinal, apenas as estações que estão em seu segmento a recebem. A principal função do bridge é filtrar pacotes entre os segmentos de redes locais.

Imagem 20

6.6 - EXERCÍCIO PROPOSTO

1 - Defina redes WAN.

_____
_____
_____

7 - ENDEREÇAMENTO DA INTERNET

Neste capítulo vamos entender como funciona o endereçamento da internet. Você já deve ter ouvido falar em IP´s. Os campos de origem e destino no cabeçalho IP contêm um endereço da internet global de 32 bits, que geralmente consiste em um identificador de rede e um identificado de host.

7.1 - CLASSES DE REDES

O endereço é codificado para tornar possível uma alocação variável de bits a fim de especificar rede e host. Essa codificação dá flexibilidade na atribuição de endereços aos hosts e permite uma mistura de rede em uma inter-rede. Logo abaixo vamos entender como são e funcionam essas classes. Na utilização do protocolo TCP/IP para comunicação algumas configurações devem ser seguidas nos equipamentos da rede.

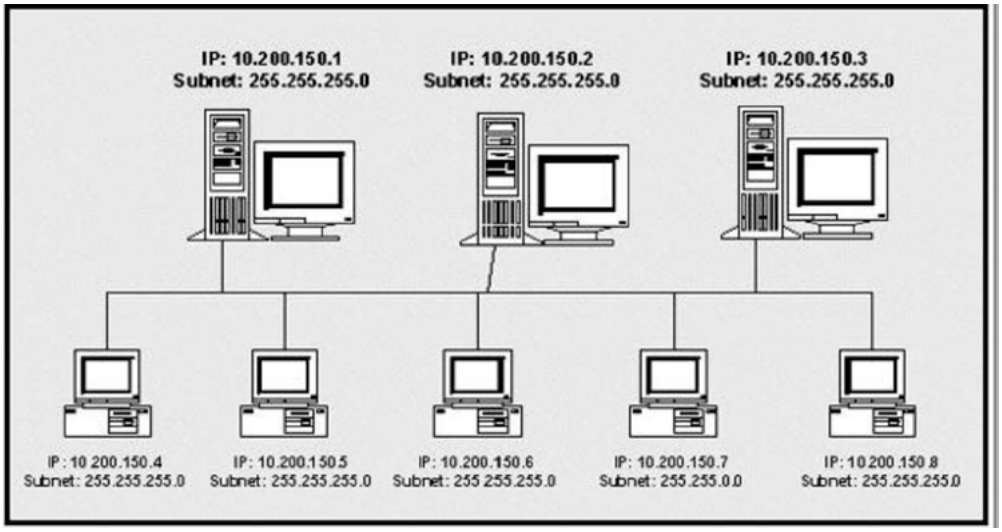


Imagem 21

A figura apresenta uma rede local de uma empresa, que pode estar conectada a outras redes ou a internet. Neste caso, dois parâmetros devem ser configurados para que a rede funcione corretamente.

- IP.
- Máscara de sub-rede (Netmask).

O número IP segue o formato de: **t.u.v.x.**, quatro números separados por ponto. Não podendo existir duas máquinas com o mesmo número IP (o que geraria conflito na rede) evitando assim que uma nova máquina não consiga conexão com a rede. O valor máximo para cada número **t.u.v.x** é de 255. Observe a explicação abaixo retirada do tutorial sobre IP´s de Júlio C.F. Battist.

"Uma parte do número IP (1, 2 ou 3 dos 4 números) é a identificação da rede, a outra parte é a identificação da máquina dentro da rede. O que define quantos dos quatro números fazem parte da identificação da rede e quantos fazem parte da identificação da máquina é a máscara de sub-rede (subnet mask). Vamos considerar o exemplo de um dos computadores da rede da figura.

Número IP: 10.200.150.1
Sub-rede: 255.255.255.0

As três primeiras partes da máscara de sub-rede (subnet) iguais a 255 indicam que os três primeiros números representam a identificação da rede e o último número é a identificação do equipamento dentro da rede. Para o nosso exemplo teríamos a rede: 10.200.150, ou seja, todos os equipamentos do nosso exemplo fazem parte da rede 10.200.150 ou, em outras palavras, o número IP de todos os equipamentos da rede começam com 10.200.150.

Neste exemplo, onde estamos utilizando os três primeiros números para identificar a rede e somente o quarto número para identificar o equipamento, temos um limite de 254 equipamentos que podem ser ligados nesta rede. Observe que são 254 e não 256, pois o primeiro número – 10.200.150.0 e o último – 10.200.250.255 não podem ser utilizados como números IP de equipamentos de rede. O primeiro é o próprio número da rede: 10.200.150.0 e o último é o endereço de broadcast: 10.200.150.255. Ao enviar uma mensagem para o endereço de broadcast, todas as máquinas da rede receberão a mensagem."

Na tabela abaixo mostramos mascaras de sub-redes:

Máscara	Número de equipamentos na rede
255.255.255.0	254
255.255.0.0	65534
255.0.0.0	16777.214

Para você saber qual IP da sua máquina na linha de comando (na máquina Windows) clique em executar -> digite cmd. Aparecerá uma tela preta, que chamamos prompt de comando e digite o comando: ipconfig /all – mostrará o IP da sua máquina. Observe a figura:

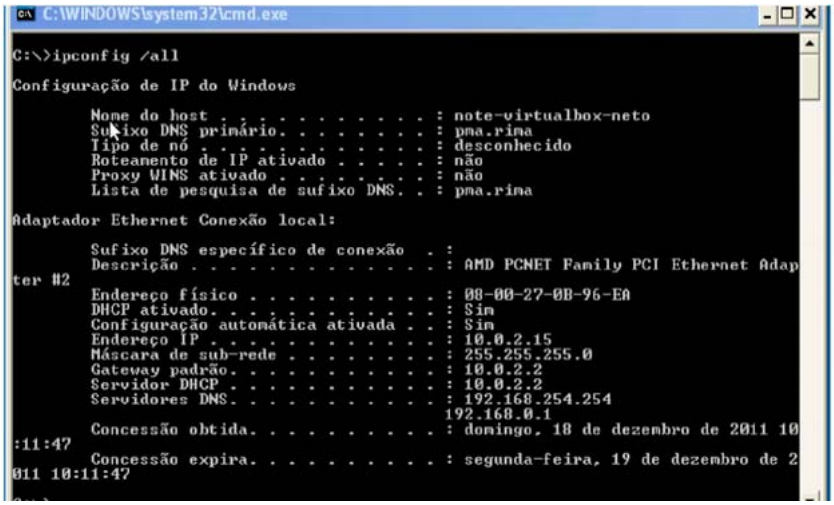

C:\WINDOWS\system32\cmd.exe
C:\>ipconfig /all
Configuração de IP do Windows
Nome do host . . . . . : note-virtualbox-neto
Sufixo DNS primário. . . . . : pma.rima
Tipo de nó . . . . . : desconhecido
Roteamento de IP ativado . . . . : não
Proxy WINS ativado . . . . . : não
Lista de pesquisa de sufixo DNS. . : pma.rima
Adaptador Ethernet Conexão local:
Sufixo DNS específico de conexão . :
Descrição . . . . . : AMD PCNET Family PCI Ethernet Adap
ter #2
Endereço físico . . . . . : 08-00-27-0B-96-EA
DHCP ativado. . . . . : Sim
Configuração automática ativada . . : Sim
Endereço IP . . . . . : 10.0.2.15
Máscara de sub-rede . . . . . : 255.255.255.0
Gateway padrão. . . . . : 10.0.2.2
Servidor DHCP . . . . . : 10.0.2.2
Servidores DNS. . . . . : 192.168.254.254
192.168.0.1
Concessão obtida. . . . . : domingo, 18 de dezembro de 2011 10
:11:47
Concessão expira. . . . . : segunda-feira, 19 de dezembro de 2
011 10:11:47

Imagem 22

Além de mostrar o IP da máquina, mostra também informações sobre as interfaces de rede que estão instaladas: placa de rede e etc.

7.2 - SISTEMA BINÁRIO

O sistema binário ou base 2 é um sistema de numeração posicional em que todas as quantidades representam-se com base em dois números, com o que se dispõe das cifras: **zero e um** (0 e 1). Os computadores digitais trabalham internamente com dois níveis de tensão, pelo que o seu sistema de numeração natural é o sistema binário (acesso, apagado). Com efeito, num sistema simples como este é possível simplificar o cálculo, com o auxílio da lógica booleana. Em computação, chama-se um dígito binário (0 ou 1) de bit, que vem do inglês Binary Digit. Um agrupamento de 8 bits corresponde a um byte (Binary Term). Um agrupamento de 4 bits é chamado de nibble.

Para obter o valor do número, multiplicamos os seus dígitos de traz para frente, baseados na potência de 2 (no numeral a potencia é 10) ou seja, 20 ,21,22,23, assim por diante. Se quisermos saber o valor decimal do número binário 11001110.

1	**1**	**0**	**0**	**1**	**1**	**1**	**0**
Multiplicamos por:	27	26	25	24	23	22	21	20
Equivale a:	128	64	32	16	8	4	2	1
Multiplicação:	1x128	1x64	0x32	0x16	1x8	1x4	1x2	0x1
Resultado	128	64	0	0	8	4	2	0
Somando:	128	64	0	0	8	4	2	0
Resultado:	206							

Outra forma: se você tiver uma calculadora científica ou utilizar a calculadora no computador, selecione a opção científica e pode transformar o binário em decimal.

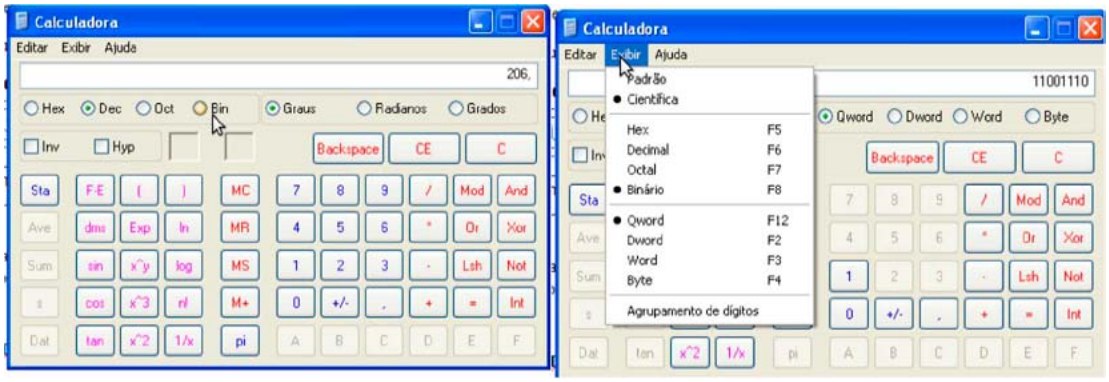


Imagem 23

7.3 - IPv 4

Um endereço IPv4 é formado por 32 bits que é o mesmo que dissermos que possui quatro octetos representados na forma decimal (Ex: 192.168.0.1). Uma parte desse endereço (bits mais significativos) indicam a rede e a outra parte (bits menos significativos) indicam-nos qual a máquina dentro da rede.

Com o objetivo de serem possíveis redes de diferentes dimensões, foram definidas cinco diferentes classes de endereços IP. Geralmente denominadas de classes: A, B, C, D e E.

Originalmente, o espaço de endereçamento IP foi dividido em estruturas de tamanho fixo designadas de "classes de endereço". As principais classes são a classe A, classe B e classe C. Com base nos primeiros bits (prefixo) de um endereço IP, conseguimos facilmente determinar rapidamente a qual a classe pertencente de um determinado endereço IP.

Na tabela abaixo apresentamos a forma resumida sobre as classes de redes IP:

Classe	Primeiro Octeto	Rede (N) Hosts (H)	Máscara	Nº de Redes	Endereços por Redes
A	1-127	N.H.H.H	255.0.0.0	$126(2^7-2)$	$16.777.214(2^{24}-2)$
B	128-191	N.N.H.H	255.255.0.0	$16.382(2^{14}-2)$	$65.534\ (2^{16}-2)$
C	192-223	N.N.N.H	255.255.255.0	$2.097.150(2^{21}-2)$	$254(2^8-2)$
D	224-239	*Multcast*	N/A	N/A	N/A
E	240-255	Reservado	N/A	N/A	N/A

N = Network
H = Hosts

Analisando as três principais classes (A, B e C) podemos verificar o seguinte:

A classe A possui um conjunto de endereços que vão desde o 1.0.0.0 até 127.0.0.0, onde o primeiro octeto (primeiros 8 bits N.H.H.H) de um endereço IP identifica a rede e os restantes 3 octetos (24 bits) irão identificar um determinado host nessa rede.

Exemplo de um endereço classe A – 120.2.1.0

A classe B possui um conjunto de endereços que vão desde o 128.0.0.0 até 191.255.0.0, onde os dois primeiros octetos (16 bits N.N.H.H.) de um endereço IP identificam a rede e os restantes 2 octetos (16 bits) irão identificar um determinado host nessa rede.

Exemplo de um endereço classe B – 152.13.4.0

A classe C possui um conjunto de endereços que vão desde o 192.0.0.0 até 223.255.255.0, onde os três primeiros octetos (24 bits N.N.N.H.) de um endereço IP identificam a rede e o restante octeto (8 bits) irão identificar um determinado host nessa rede.

Exemplo de um endereço classe C – 192.168.10.0

Quanto às classes D e E, elas existem por motivos especiais: a primeira é usada para a propagação de pacotes especiais para a comunicação entre os computadores, enquanto que a segunda está reservada para aplicações futuras ou experimentais.

Vale frisar que há vários blocos de endereços reservados para fins especiais. Por exemplo, quando o endereço começa com 127, geralmente indica uma rede "falsa", isto é, inexistente, utilizada para testes. No caso do endereço 127.0.0.1, este sempre se refere à própria máquina, ou seja, ao próprio host, razão esta que o leva a ser chamado de local host. Já o endereço 255.255.255.255 é utilizado para propagar mensagens para todos os hosts de uma rede de maneira simultânea.

7.4 - ENDEREÇOS IP PRIVADOS[5]

5 - IP - sigla para Internet Protocol.

Há conjuntos de endereços das classes A, B e C que são privados. Isto significa que eles não podem ser utilizados na internet, sendo reservados para aplicações locais. São, essencialmente, estes:

- Classe A: 10.0.0.0 à 10.255.255.255.
- Classe B: 172.16.0.0 à 172.31.255.255.
- Classe C: 192.168.0.0 à 192.168.255.255.

Suponha então que você tenha que gerenciar uma rede com cerca de 50 computadores. Você pode alocar para estas máquinas endereços de 192.168.0.1 até 192.168.0.50, por exemplo. Todas elas precisam de acesso à internet. O que fazer? Adicionar mais um IP para cada uma delas? Não. Na verdade, basta conectá-las a um servidor ou equipamento de rede - como um roteador - que receba a conexão à internet e a compartilhe com todos os dispositivos conectados a ele. Com isso, somente este equipamento precisará de um endereço IP para acesso à rede mundial de computadores.

7.5 - IP ESTÁTICO E IP DINÂMICO

IP estático (ou fixo) é um endereço IP dado permanentemente a um dispositivo, ou seja, seu número não muda, exceto se tal ação for executada manualmente. Como exemplo, há casos de assinaturas de acesso à internet via ADSL onde o provedor atribui um IP estático aos seus assinantes. Assim, sempre que um cliente se conectar, usará o mesmo IP.

O IP dinâmico, por sua vez, é um endereço que é dado a um computador quando este se conecta a rede, mas que muda toda vez que há conexão. Por exemplo, suponha que você conectou seu computador à internet hoje. Quando você conectá-lo amanhã, lhe será dado outro IP. Para entender melhor, imagine a seguinte situação: uma empresa tem 80 computadores ligados em rede. Usando IP´s dinâmicos, a empresa disponibiliza 90 endereços IP para tais máquinas. Como nenhum IP é fixo, um computador receberá, quando se conectar, um endereço IP destes 90 que não estiver sendo utilizado. É mais ou menos assim que os provedores de internet trabalham.

O método mais utilizado na distribuição de IP´s dinâmicos é o protocolo DHCP (Dynamic Host Configuration Protocol).

7.6 - ENDEREÇAMENTO

Os endereços IP identificam cada micro na rede. A regra básica é que cada micro deve ter um endereço IP diferente e todos devem usar endereços dentro da mesma faixa.
O endereço IP é dividido em duas partes. A primeira identifica a rede à qual o computador está conectado e a segunda identifica o computador (chamado de host) dentro da rede.

7.6.1 - MODOS DE ENDEREÇAMENTO

Usualmente um endereço refere-se a um único sistema Unicast. Pode endereçar todas as entidades dentro de um domínio Broadcast. Pode endereçar um subconjunto de entidades dentro de um domínio Multcast.

7.6.2 - SENTIDO DE TRANSMISSÃO OU MODO DE OPERAÇÃO

7.6.2.1 - SIMPLEX

O sinal vai apenas da origem (previamente determinada) para o destino (previamente determinado).

7.6.2.2 - HALF DUPLEX OU SEMIDUPLEX

O sinal pode ser transmitido da origem para o destino e vice-versa, mas não é ao mesmo tempo.

7.6.2.3 - DUPLEX OU FULL DUPLEX

Os sinais podem ser transmitidos ao mesmo tempo, entre as duas extremidades que estão se comunicando, em ambos sentidos.

7.6.3 - CONTROLE DE ERROS

Controlam perdas e erros de transmissão, a origem insere bits para detecção de erros, o receptor verifica a ocorrência desses erros. Se nada for encontrado o pacote é aceito, se tem erros, o pacote é descartado.

7.7 - CONTROLE DE FLUXO

Coloca os pacotes recebidos em ordem, caso eles tenham chegado, com erros e fora de ordem, tipicamente enviando para o transmissor uma informação de recebimento, informando que o pacote foi recebido com sucesso.

7.8 - EXERCÍCIO PROPOSTO

1 - Qual comando utilizado no ambiente Windows para ver o IP da máquina?

_____
_____
_____

8 – REDES WIRELESS6

As redes sem fio ou *Wireless* (WLAN´s) surgiram da mesma forma que muitas outras tecnologias, no meio militar. Havia a necessidade de implementação de um método simples e seguro para troca de informações em ambiente de combate. O tempo passou e a tecnologia evoluiu, deixando de ser restrito ao meio militar e se tornou acessível a empresas, faculdades e ao usuário doméstico. Nos dias de hoje podemos pensar em redes wireless como uma alternativa bastante interessante em relação às redes cabeadas, embora ainda com custo elevado. Suas aplicações são muitas e variadas e o fato de ter a mobilidade como principal característica, tem facilitado sua aceitação, principalmente nas empresas.

A evolução dos padrões oferecendo taxas de transmissão comparáveis a Fast Ethernet, por exemplo, torna as redes wireless uma realidade cada vez mais presente.

WLAN´s usam ondas de radio para transmissão de dados. Comumente podem transmitir na faixa de frequência 2.4 Ghz (não licenciada) ou 5 Ghz.

8.1 - PADRÕES

Como WLAN´s usam o mesmo método de transmissão das ondas de rádio AM/FM, as leis que as regem são as mesmas destes. O FCC (*Federal Comunications Comission*) regula o uso dos dispositivos WLAN. O IEEE *(Institute of Eletrical and Eletronic Engineers*) é responsável pela criação e adoção dos padrões operacionais. Citamos os mais conhecidos:

IEEE 802.11	- Criado em 1994, foi o padrão original. - Oferecia taxas de transmissão de 2 Mbps. - Caiu em desuso com o surgimento de novos padrões.
IEEE 802.11b	- Taxas de transmissão de 11Mbps. - Largamente utilizada hoje em dia. - Opera em 2.4Ghz. - Alcance de até 100m indoor e 300m outdoor. - Mais voltado para aplicações indoor. - Tende a cair em desuso com a popularização do 802.11g.
IEEE 802.11ª	- Taxas de transmissão de 54Mbps. - Alcance menor do que a 802.11b. - Opera em 5Ghz. - Alcance de até 60m indoor e 100m outdoor. - Mais voltado para aplicações indoor. - Seu maior problema é a não compatibilidade com dispositivos do padrão b, o que prejudicou e muito sua aceitação no mercado.
IEEE 802.11g	- Taxas de transmissão de 54Mbps podendo chegar em alguns casos a 108Mbps. - Opera em 2.4Ghz. - Mais voltado para aplicações indoor. - Reúne o melhor dos mundos a e b (alcance x taxa).

6 - *Wireless (wire = fio, less = sem)* significa um sistema de antenas interligadas entre si, que transmitem informações via ondas de rádio. Essa tecnologia vem sendo amplamente adotada por se tratar de uma solução que possibilita alta velocidade a um custo semelhante ao da conexão discada.

IEEE 802.16a	- Criado em 2003. - Popularmente conhecido como Wi-Max. - Voltado exclusivamente para aplicações outdoor. - Alcance de até 50Km. - Taxas de transmissão de até 280Mbps.

8.2 – TÉCNICAS DE TRANSMISSÃO

WLAN´s usam uma técnica de transmissão conhecida como difusão de espectro (*Spread Spectrum*). Essa técnica se caracteriza por larga banda e baixa potência de sinal. São sinais difíceis de detectar e mesmo interceptar sem o equipamento adequado. Existem dois tipos de tecnologias de Spread Spectrum regulamentadas pelo FCC: *Direct Sequence Spread Spectrum* (DSSS) e *Frequency Hopping Spread Spectrum* (FHSS).

DSSS	- Menos resistente a interferência. - Compatibilidade com equipamentos de padrões anteriores. - Taxa de Transmissão de 11 Mbps. - Menor segurança. - Possui 11 canais, mas destes somente 3 são não interferentes e os efetivamente usados para transmissão – Canais : 1, 6 e 11
FHSS	- Mais resistente à interferência. - Não possui compatibilidade com equipamentos de padrões anteriores. - Taxa de transmissão de 2Mbps. - Maior segurança. - 79 canais disponíveis para transmissão.

8.3 – ELEMENTOS DE HARDWARE

Na tabela a seguir descrevemos os componentes de uma WLAN.

PC Card	- Usado somente em notebooks. - Serve para conectar o notebook a rede Wireless. - Possui antena interna embutida.
Placas PCI	- Usado somente em desktops. - Serve para conectar o desktop a rede Wireless. - Possui antena externa acoplada a saída da placa.
Adaptadores USB	- Pode ser usado em notebooks ou desktops. - Serve para conectar o notebook ou desktop a rede Wireless. - Possui antena interna embutida.
Pontos de Acesso	- Concentra todo o tráfego da rede Wireless além das conexões oriundas dos clientes. - Possui um identificador que identifica a rede chamado SSID. - Interface entre a rede wireless e a rede cabeada por possuir porta UTP 10 ou 100Mbps. - Possui antena interna embutida. - Suporta a conexão de antenas externas, na maioria dos casos.

Pontes *Wireless* Workgroup	- Agrupa vários clientes LAN e transforma essa LAN em único cliente WLAN. - Recomendado em situações em que um pequeno grupo de usuários necessita de acesso à rede principal. - O número máximo de estações que pode ser conectado está compreendido entre 8 e 128, dependendo do fabricante.
Pontes *Wireless*	- Conecta duas ou mais redes. - Compreende 4 modos de operação: Root, Non-Root, Access Point e Repeater. - Possui a capacidade de formação de backbone Wireless através de 2 PC Cards.
Gateways	- Conecta um pequeno número de dispositivos Wireless a internet ou outra rede - Possui uma porta WAN e várias portas LAN. Geralmente tem um hub ou switch embutido e possui as funcionalidades de um Ponto de Acesso.
Antenas	- Podem ser conectadas a pontos de acesso ou a máquinas-clientes para aumentar o ganho do sinal e assim melhorar a transmissão de dados. - Podem ser direcionais ou omnidirecionais.

8.4 – TIPOS DE WLAN

Uma WLAN pode ser utilizada tanto na forma indoor quanto na forma outdoor.

8.4.1 - INDOOR

Dizemos que uma WLAN é indoor quando o sinal está sendo transmitido em ambiente fechado normalmente na presença de muitos obstáculos, um escritório é um bom exemplo. Não há necessidade de visada direta entre as antenas para que haja comunicação. O alcance é pequeno em torno de até 300 metros. Podem ter a presença de um ponto de acesso ou não.

ADHOC	☐ Não existem Pontos de Acesso (AP). ☐ Comunicação feita cliente – cliente. ☐ Não existe canalização do tráfego. ☐ A performance diminui a medida que novos clientes são acrescentados. ☐ Suporta no máximo 5 clientes para uma performance aceitável com tráfego leve.
Infraestrutura	☐ Necessidade de um Ponto de Acesso (AP). ☐ Comunicação cliente – cliente não é permitida. Toda a comunicação é feita com o AP. ☐ Centralização do tráfego. Todo o tráfego da rede passa pelo AP. ☐ Compreende dois modos de operação: BSS (Basic Service Set), ESS (Extended Service Set).

BSS – consiste de um ponto de acesso ligado à rede cabeada e, um ou mais clientes Wireless. Quando um cliente quer se comunicar com outro ou com algum dispositivo na rede cabeada deve usar o ponto de acesso para isso. O BSS compreende uma simples célula ou área de RF e tem somente um identificador (SSID). Para que um cliente possa fazer parte da célula ele deve estar configurado para usar o SSID do ponto de acesso.

ESSS – são dois sistemas BSS conectados por um sistema de distribuição, seja ele LAN, WAN, Wireless ou qualquer outro. Necessita, portanto de dois pontos de acesso. Permite roaming entre as células. Não necessita do mesmo SSID em ambos os BSS.

8.4.2 - OUTDOOR

Dizemos que uma WLAN é outdoor, quando o sinal está sendo transmitido ao ar livre, uma comunicação entre dois prédios é um bom exemplo. As antenas ficam nos topos dos prédios e para que haja comunicação é necessário haver visada direta entre elas. Possui longo alcance podendo chegar a vários quilômetros.

8.5 - APLICAÇÕES

Hoje em dia a utilização das WLAN´s deixou de ser restrito a grandes empresas ou faculdades. Com os preços dos equipamentos mais acessíveis, elas acabaram atraindo a atenção do usuário comum devido a sua ampla gama de possibilidades de utilização. Vejamos os mais comuns.

8.5.1 - EXPANSÃO DA REDE CABEADA

Podem ocorrer casos em que a expansão de uma rede seja inviável devido ao custo proibitivo da estrutura necessária para o cabeamento adicional (cabos, contratação de instaladores e eletricistas), ou casos onde a distância pode ser muito grande (acima de 100 metros) para se usar cabos CAT5, como em uma loja de departamentos por exemplo. Em tais casos WLAN´s certamente serão uma alternativa de baixo custo e de fácil implementação.

8.5.2 - CONEXÃO ENTRE PRÉDIOS

É muito comum uma empresa ter escritórios em prédios diferentes que necessitam estar conectados a mesma infraestrutura de rede. O que era comum para atingir esse objetivo era alugar linhas privadas de uma companhia de telefonia ou utilizar passagens subterrâneas para a infra de cabos. Esses métodos eram dispendiosos e demorados para implementar. WLAN´s surgem como uma alternativa de rápida implementação e de baixo custo comparados aos métodos tradicionais. A comunicação entre os prédios se torna possível graças as antenas e aos equipamentos wireless de cada um deles.

A comunicação pode ser realizada basicamente de duas formas no que se refere à conectividade prédio a prédio.

- PTP (Ponto a Ponto) - são conexões wireless entre dois prédios e usam antenas direcionais de alto ganho em cada um deles.

- PTMP (Ponto Multiponto) - são conexões Wireless entre três ou mais prédios, sendo que um atua como central. No prédio central usa-se uma antena omnidirecional e nos outros, antenas direcionais.

Obs.: Em ambos os tipos de comunicação é fundamental haver visada direta entre as antenas.

8.5.3 - SERVIÇOS DE ÚLTIMA MILHA

Esse tipo de serviço é largamente utilizado por provedores de internet para levar o acesso à internet até uma localidade remota que não dispõe dos meios tradicionais de acesso em banda larga (xDSL e cable modem).

A grande vantagem é que os custos de instalação são bem menores se comparados aos métodos tradicionais, mas sempre tem que ser levado em conta a situação e a relação

custo X benefício. Da mesma forma que provedores xDSL têm problemas com distâncias grandes a partir do escritório central e provedores de cabos tem problemas com a meio sendo compartilhado pelos usuários, provedores Wireless tem problemas com telhados, arvores, montanhas, torres e muitos obstáculos.

Embora provedores Wireless não tenham uma solução a prova de falhas, eles podem levar seus serviços até onde outros de tecnologias tradicionais não conseguem.

8.5.4 - MOBILIDADE

Uma das principais características da tecnologia Wireless é a mobilidade, que por sua vez pode acarretar em um aumento real de produtividade em determinados casos, tais como, uma loja de departamentos.

Em uma loja de departamentos os funcionários responsáveis por catalogar os produtos, podem estar munidos de scanners de mão wireless e estes por sua vez estarem conectados a um computador central por meio de uma rede Wireless. Existe uma economia de tempo brutal nesse caso e um consequente aumento de produtividade porque não há necessidade da entrada de dados manual através de um terminal ligado ao computador central por meio de cabos. Os dados são transferidos automaticamente.

8.5.6 - ESCRITÓRIOS MÓVEIS

Imagine que você tem uma empresa de treinamento e gostaria de divulgar seus serviços ao público em geral. Sua empresa possui um trailer e seu desejo é usá-lo como uma sala de aula móvel com acesso a internet e poder também divulgar serviços oferecidos pela sua empresa. Uma boa maneira de viabilizar isso seria com a tecnologia Wireless. Para tal seria necessário uma antena omnidirecional posicionada no topo do prédio da sua empresa e outra direcional de alto ganho no alto do veículo, além dos computadores e mais alguns equipamentos. Lembrando que a sua mobilidade estaria restrita a área de cobertura da antena omnidirecional.

8.5.7 - HOSTSPOTS

São pontos de acesso Wireless que permitem ao usuário conectar-se na internet estando em locais públicos como aeroportos, shoppings, hotéis, cafeterias e outros.
Bastaria um laptop com um PCCard e uma conta de acesso da provedora do serviço para estar navegando na internet nesses locais, não esquecendo que o usuário é cobrado pelo uso do serviço.

8.5.8 - USO DOMÉSTICO

Na sua casa você pode ter mais de um computador que necessita de acesso à internet. Normalmente você necessitaria levar cabos para esses computadores adicionais a partir do hub em que também está conectado o computador que acessa a internet.

Com a tecnologia Wireless a passagem de cabos se torna desnecessária (o que muitas vezes pode resultar em significativa economia de tempo) e se você tiver um notebook você ganha mobilidade. Imagine poder acessar a internet do seu notebook estando em qualquer cômodo da casa? Ou ainda no caso do computador, mudá-lo do quarto para a sala se houver necessidade, sem se preocupar em passar cabos?

No que se refere ao custo, instalar uma rede Wireless ainda é bem mais caro que uma rede cabeada, mas os benefícios compensam. A tabela abaixo ilustra a diferença de custo (preços médios) para dois computadores (um notebook e um desktop), distante 15m do hub ou switch. O notebook e o desktop já possuem placa de rede.

8.6 - PONTOS DE ACESSO (AP)

Ponto de acesso como o próprio nome sugere, funcionam como ponto de entrada de uma rede para um cliente. É um dispositivo half-duplex com funcionalidades similares aos switches Ethernet modernos, com a diferença de ser sem fio.

É composto por uma ou duas antenas de ganho baixo (normalmente 5dBi no máximo) que na maioria dos casos pode ser removida para a conexão de antenas com ganho maior e uma porta Ethernet para conexão a rede cabeada. São considerados portais pelo fato de conectarem clientes de uma rede 802.11(WLAN) a uma rede 802.3 (Ethernet) ou 802.5 (Token Ring). Em uma rede com AP, todo o fluxo de dados passa por ele. Normalmente são utilizados para aplicações indoor.

8.6.1 – MODOS DE OPERAÇÃO

Pontos de acesso podem se comunicar com seus clientes wireless, com a rede Ethernet e com outros pontos de acesso. Existem três modos de operação:

- **Modo Root.**
- **Modo Repetidor.**
- **Modo Ponte.**

8.6.1.1 – MODO ROOT

É utilizado quando o AP é conectado a um backbone Ethernet. Este é o modo de operação padrão. Neste modo, AP´s que estão conectados ao mesmo segmento Ethernet, podem se comunicar por meio deste. AP´s se comunicam para coordenar funcionalidades de roaming, tais como reassociação. Clientes Wireless localizados em células diferentes podem se comunicar por meios de seus respectivos AP´s, através do segmento Ethernet.

8.6.1.2 – MODO PONTE

Neste modo o AP atua como se fosse uma ponte Wireless ligando dois segmentos Ethernet. A finalidade de uma ponte é isolar dois segmentos de rede e dessa forma impedir que o tráfego não endereçado as máquinas de um determinado segmento atinjam o mesmo, evitando a sobrecarga daquele segmento. O AP´s nesse modo fazem o mesmo só que a ligação entre eles é sem fio. Existem poucos AP´s no mercado com essa funcionalidade, devido ao fato de que essa característica aumenta substancialmente o custo do equipamento. Diferentemente do modo Root, nesse modo os clientes não se associam ao AP.

8.6.1.3 – MODO REPETIDOR

Neste modo um AP atua no modo Root enquanto que o outro atua como repetidor. Os clientes se associam ao AP repetidor que por sua vez é um cliente do AP Root. A ligação entre eles forma um link Wireless dentro de uma estrutura cabeada. Este modo não é muito utilizado porque existem algumas desvantagens:

Os clientes ligados ao AP repetidor experimentam baixo throughput e altos tempos de latência nessa configuração, devido ao fato de que ambos os AP´s se comunicam com os clientes através do mesmo link Wireless.

O alcance na qual os clientes podem se associar ao AP repetidor é reduzida drasticamente.

8.7 - REDES SEM FIO (WIRELESS)

Como já sabemos as redes sem fio (Wireless), também conhecidas como IEEE 802.11, Wi-Fi ou WLAN´s, são redes que utilizam sinais de rádio para a sua comunicação.
Este tipo de rede define duas formas de comunicação:

• **Modo Infraestrutura** - normalmente o mais encontrado, utiliza um concentrador de acesso (Access Point ou AP).
• **Modo Ponto a Ponto (Ad-hoc) -** permite que um pequeno grupo de máquinas se comunique diretamente, sem a necessidade de um AP.

Estas redes ganharam grande popularidade pela mobilidade que proveem aos seus usuários e pela facilidade de instalação e uso em ambientes domésticos e empresariais, hotéis, conferências, aeroportos e etc.

8.7.1 - QUAIS SÃO OS RISCOS DO USO DE REDES SEM FIO?

Embora esse tipo de rede seja muito conveniente, existem alguns problemas de segurança que devem ser levados em consideração pelos seus usuários: estas redes utilizam sinais de rádio para a comunicação e qualquer pessoa com um mínimo de equipamento poderá interceptar os dados transmitidos por um cliente da rede sem fio (como notebooks, PDAs, estações de trabalho e etc.); por serem bastante simples de instalar, muitas pessoas estão utilizando redes desse tipo em casa, sem nenhum cuidado adicional, e até mesmo em empresas, sem o conhecimento dos administradores de rede.

8.7.2 - QUE CUIDADOS DEVO TER COM UM CLIENTE DE UMA REDE SEM FIO?

Vários cuidados devem ser observados quando se pretende conectar a uma rede sem fio como cliente, seja com notebooks, PDA´s, estações de trabalho e etc.

Considerar que, ao conectar a uma WLAN, você estará conectando-se a uma rede pública e, portanto, seu computador estará exposto a ameaças. É muito importante que você tome os seguintes cuidados com o seu computador:

• Instalar um firewall pessoal.
• Instalar e manter atualizado um bom programa antivírus.
• Atualizar as assinaturas do antivírus diariamente.
• Aplicar as últimas correções em seus softwares (sistema operacional, programas que utiliza e etc.).
• Desligar compartilhamento de disco, impressora, etc.
• Desabilitar o modo Ad hoc. Utilize esse modo apenas se for absolutamente necessário e desligue-o assim que não precisar mais.
• Sempre que possível usar WEP (Wired Equivalent Privacy), que permite criptografar o tráfego entre o cliente e o AP. Fale com o seu administrador de rede para verificar se o WEP está habilitado e, se a chave é diferente daquelas que acompanham a configuração padrão do equipamento. O protocolo WEP possui diversas fragilidades e deve ser encarado como uma camada adicional para evitar a escuta não autorizada.
•Verificar com seu provedor de rede sem fio sobre a possibilidade de usar WPA (Wi-Fi Protected Access) em substituição ao WEP, uma vez que este padrão pode aumentar significativamente a segurança da rede. Esta tecnologia inclui duas melhorias em relação ao protocolo WEP que envolvem melhor criptografia para transmissão de dados e autenticação de usuário. Mesmo que seu equipamento seja mais antigo, é possível que exista uma atualização para permitir o uso de WPA.
• Considerar o uso de criptografia nas aplicações, como por exemplo, o uso de PGP para o envio de e-mails, SSH para conexões remotas ou ainda o uso de VPN´s.
• Evitar o acesso a serviços que não utilizem conexão segura, ao usar uma rede sem fio em local público. Por exemplo, se for necessário ler e-mails ou acessar a intranet da sua empresa, dê preferência a serviços que usem criptografia.
• Habilitar a rede sem fio somente quando for usá-la e desabilitá-la após o uso. Algumas estações de trabalho e notebooks permitem habilitar e desabilitar o uso de redes sem fio através de comandos ou botões específicos. No caso de notebooks

com cartões PCMCIA, insira o cartão apenas quando for usar a rede e retire-o ao terminar de usar.

8.7.3 - QUE CUIDADOS DEVO TER AO MONTAR UMA REDE SEM FIO DOMÉSTICA?

Pela conveniência e facilidade de configuração das redes sem fio, muitas pessoas têm instalada estas redes em suas casas. Nestes casos, além das preocupações com os clientes da rede, também são necessários alguns cuidados na configuração do AP.

Ter em mente que, dependendo da potência da antena de seu AP, sua rede doméstica pode abranger uma área muito maior que apenas a da sua casa. Com isto sua rede pode ser utilizada sem o seu conhecimento ou ter seu tráfego capturado por vizinhos ou pessoas que estejam nas proximidades da sua casa; mudar configurações padrão que acompanham o seu AP. Alguns exemplos são:

- Alterar as senhas.
- Alterar o SSID (Server Set ID).
- Desabilitar o broadcast de SSID.
- Permitir que um computador se conecte ao AP para alterar as configurações apenas através da rede cabeada, se esta opção estiver disponível. Desta maneira um possível atacante externo (via rede sem fio) não poderá acessar o AP diretamente para promover mudanças na configuração. Verifique a documentação do seu AP sobre como efetuar estas mudanças, caso estejam disponíveis.
- Verificar se seus equipamentos já suportam WPA (Wi-Fi Protected Access) e utilizá-lo sempre que possível. Esta tecnologia é mais recente e inclui melhorias em relação ao protocolo WEP para prover uma segurança adicional contra acesso e escuta de tráfego não autorizado. Lembre-se que atualizações para WPA estão disponíveis para a maior parte dos equipamentos mais antigos.
- Caso o WPA não esteja disponível, usar sempre que possível WEP (Wired Equivalent Privacy), para criptografar o tráfego entre os clientes e o AP. Vale lembrar que o protocolo WEP possui diversas fragilidades e deve ser encarado como uma camada adicional para evitar a escuta não autorizada.
- Se for utilizar WEP, trocar as chaves que acompanham a configuração padrão do equipamento. Procure usar o maior tamanho de chave possível (128 bits); desligar seu AP quando não estiver usando sua rede.

8.7.4 - EXPLICAÇÃO SOBRE SSID

O SSID é um identificador de uma determinada célula. Para que possa haver associação com um AP, o cliente deve saber o SSID daquela célula. O cliente pode fazer isso de duas formas:

- O AP divulga o SSID, dessa forma o cliente se conecta ao AP de forma automática, bastando apenas estar operando no mesmo canal do AP.
- O AP não divulga o SSID. Nesse caso a associação só ocorre se o cliente estiver configurado com o SSID do AP. Isso é uma medida de segurança. Nem todos os AP´s tem essa característica.

8.8 - EXERCÍCIO PROPOSTO

1 - O que são Hotspots?

_____
_____
_____

9 – COMPUTAÇÃO CLIENTE – SERVIDOR

É importante conhecer a computação cliente-servidor, pois na maioria, se não em todas, esse modelo é aplicado. O modelo está cada vez mais substituindo a computação centralizada, que é dominada pelos *mainframes*. Um ambiente cliente-servidor é preenchido por clientes e servidores, onde as máquinas clientes, geralmente PC´s, estações de trabalho. O objetivo é facilitar a utilização de ferramentas pelo cliente. As interfaces Microsoft, Mac OS X são exemplos de ambiente para clientes. Cada servidor neste ambiente fornece uma serie de serviços compartilhados do usuário para os clientes. Um tipo conhecido por todos, é o servidor de banco de dados. O servidor permite que muitos clientes compartilhem o acesso ao mesmo banco de dados.

9.1 - A REDE

No ambiente cliente-servidor a rede é fundamental, pois a computação cliente-servidor é distribuída; usuários, aplicações, recursos estão distribuídos conforme as regras das empresas e ligadas por uma rede LAN ou WAN ou ainda por uma inter-rede.

Conforme STALLINGS, p. 137 cita em seu livro "Redes e Sistemas de Comunicação de Dados":

> • Existe uma grande dependência de levar aplicações amigáveis ao usuário para o próprio sistema do usuário. Isso lhe da bastante controle sobre o tempo e o estilo de uso do computador, o que propicia aos gerentes no nível de departamento a capacidade de serem responsivos[7] às suas necessidades locais.
> • Embora as aplicações estejam dispersas, existe uma ênfase na centralização do banco de dados corporativos, e em muitas funções de gerenciamento de rede e utilitários. Isso permite que a gerencia coorporativa mantenha controle geral do investimento do capital total nos sistemas de computação e informação.
> • Existe um compromisso, tanto pelas organizações de usuários quanto fornecedores, em relação aos sistemas abertos e modulares. Isso significa que o usuário tem maior escolha na seleção de produtos e na mistura de equipamentos de diversos fornecedores.
> • A rede é fundamental para a operação. Assim, o gerenciamento e a segurança da rede possuem uma alta prioridade na organização e na operação dos sistemas de informação.

A computação cliente-servidor é uma nova abordagem técnica para a computação distribuída, e é também responsiva, na verdade ela cria novos meios de organização da empresa.

9.2 – EVOLUÇÃO DA COMPUTAÇÃO – CLIENTE-SERVIDOR

O crescimento desse estilo de computação teve seu início no nível de grupo de trabalho e departamento. Os gerentes departamentais perceberam que contar com aplicações centrais, baseadas em mainframes, não traziam respostas rápidas às demandas da organização. A distribuição de PC´s permitiu que os trabalhadores tivessem poder de computação e dados ao seu comando, permitindo aos gerentes de departamentos acesso as aplicações rapidamente. E para efetuar essa junção entre acesso a banco de dados aplicações através dos PC´s, a solução foi computação cliente-servidor a nível de departamento. Partindo do sucesso desse modelo cliente-servidor nos departamento, introduziu a formação da

7 - Responsivo - que envolve resposta", "Que responde", "Que se autorresponsabiliza", "Que recepciona".

computação cliente-servidor em nível de organização.

9.3 - APLICAÇÕES CLIENTE-SERVIDOR

No modelo cliente-servidor o sistema operacional é o software básico rodando na plataforma de hardware. As plataformas e os sistemas operacionais do cliente e do servidor podem ser diferentes, desde que determinado cliente e servidor compartilhem os mesmos protocolos de comunicação e admitam as aplicações. E o software que permite que cliente e servidor operem de forma integrada. Segundo STALLINGS, p.139:

> O exemplo desse tipo de software é o TCP/IP. Naturalmente, a finalidade de todo esse software de suporte (comunicação e sistema operacional) é fornecer uma base para aplicações distribuídas. O ideal é que as funções reais executadas pela aplicação se dividam entre cliente e servidor de modo que otimizem os recursos de plataforma e rede, e que otimizem a capacidade de os usuários realizarem diversas tarefas e cooperem entre si com a utilização de recur

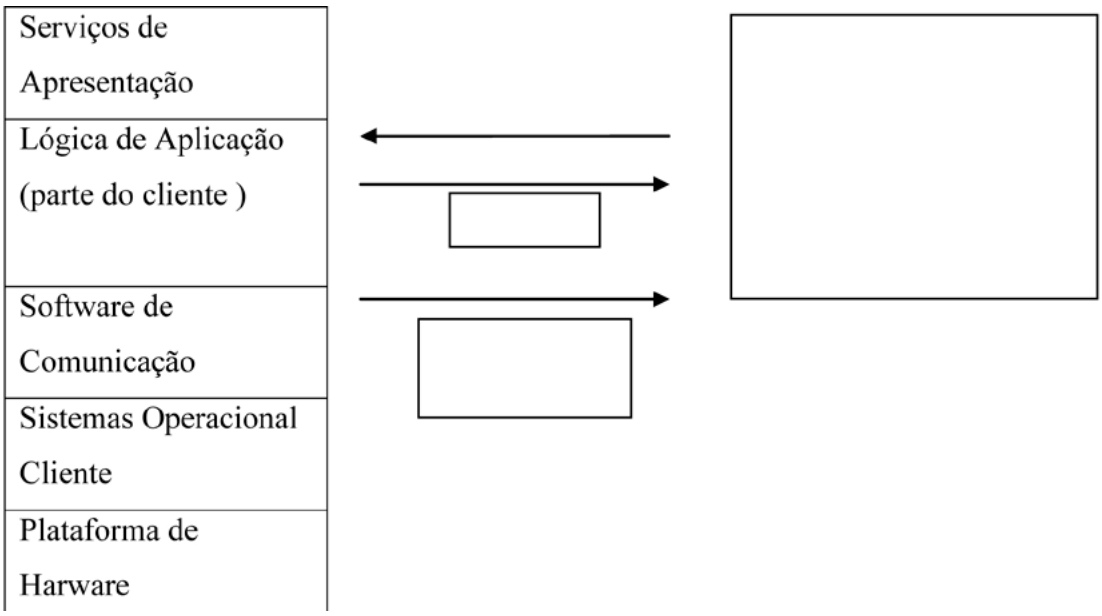


Imagem 24

9.4 - TERMINOLOGIA DE CLIENTE-SERVIDOR

9.4.1 - APPLICATION PROGRAMMING INTERFACE (API)

Um conjunto de funções e chamadas de programas e que permite a comunicação entre cliente e servidores.

9.4.2 - CLIENTE

Um solicitante de informações em rede, normalmente um PC ou estação de trabalho, que pode consultar o banco de dados e /ou outras informações de um servidor.

9.4.3 - MIDDLEWARE

Um conjunto de drivers, API´s ou outro software, que melhora a conectividade entre uma aplicação cliente e um servidor.

9.4.4 - BANDO DE DADOS RELACIONAL

Um banco de dados em que o acesso às informações limita-se à seleção das linhas que satisfazem todos os critérios de busca.

9.4.5 - SERVIDOR

Um computador, normalmente uma estação de trabalho poderosa ou um mainframe, que abriga informações para manipulação por cliente em rede.

9.4.6 - STRUCTURED QUERY LANGUAGE (SQL)

Uma linguagem desenvolvida pela IBM e padronizada pela ANSI para endereçar, criar, atualizar ou consultar banco de dados relacionais.

9.5 - CLASSES DE APLICAÇÕES CLIENTE-SERVIDOR

Na estrutura da computação cliente-servidor, existe um espectro das implementações que divide o trabalho entre cliente-servidor. Essa distribuição de dados e processo da aplicação depende da natureza das informações solicitadas ao banco e o tipo de aplicação permitidos, da disponibilidade do equipamento e dos padrões de uso dentro da organização. Algumas classes de aplicações de banco de dados.

9.5.1 - PROCESSAMENTO BASEADO EM HOST

Esse tipo de processamento não é uma aplicação cliente-servidor. Refere-se, no entanto ao ambiente de mainframe tradicional em que todo ou quase todo processamento é feito em um host central. Sendo a interface com o usuário por meio de um terminal "burro".

9.5.2 - PROCESSAMENTO BASEADO EM SERVIDOR

Essa classe é a mais simples da configuração cliente-servidor, onde o cliente é responsável por oferecer uma interface gráfica com o usuário, enquanto quase todo processamento é feito no servidor.

9.5.3 - PROCESSAMENTO BASEADO EM CLIENTE

Nessa classe, praticamente todo processamento poderá ser feito no cliente, tendo a exceção das rotinas de validação de dados e outras funções do bando de dados que é bem melhor executada no servidor. Essa talvez seja a mais utilizada atualmente, permitindo que o usuário empregue as aplicações ajustando às necessidades locais.

9.5.4 - PROCESSAMENTO COOPERATIVO

O processo cooperativo, é feito utilizando um padrão otimizado, reunindo os pontos fortes das máquinas-cliente, servidor e da distribuição de dados. Não é fácil a configuração, porém, com o tempo apresenta um maior ganho de produtividade e uma maior eficiência da rede.

9.6 - EXERCÍCIO PROPOSTO

1 - Defina Servidor.

_____

_____

_____

10 – CAMADA DE TRANSPORTE

Antes de apresentarmos a camada de transporte, veremos informações sobre as camadas físicas, enlace de dados e rede. As informações que seguem foram retiradas do livro "Redes de Computadores", de Andrew S. Tanenbaum.

10.1 - CAMADA FÍSICA

Este é o próprio meio físico da rede. Assim qualquer comunicação deverá passar forçosamente por este meio. Nesta camada estão incluídos todos os dispositivos físicos da rede; cabos, placas de rede e etc.

10.2 - CAMADA ENLACE DE DADOS

Alguns meios físicos de comunicação (Ex: linhas telefônicas), requerem o uso de técnicas específicas para que se possam transmitir dados entre sistemas, mesmo quando sob condições de taxas de erro relativamente altas. Essas técnicas são usadas em procedimentos de controle de enlace de dados.

Esta camada tem as seguintes funções:

1 - Detectar e, possivelmente, corrigir erros nas camadas de meios físicos.

2 - Fornecer à camada de rede a capacidade de pedir estabelecimento de circuitos de dados na camada (Capacidade de controlar o chaveamento de circuitos).

O propósito desta camada é fornecer os meios funcionais e de procedimento para ativar, manter e desativar uma ou mais conexões de enlace de dados entre entidades da camada de rede.

10.3 - CAMADA DE REDE

Esta camada é a responsável pelo encaminhamento dos pacotes entre os hosts, ou seja, tem por função encontrar o caminho mais curto e menos congestionado entre os computadores. Isto é conseguido pelo protocolo IP. Esta camada é ainda responsável pelo envio dos pacotes.

10.4 - CAMADA DE TRANSPORTE

A camada de transporte não é simplesmente outra camada. Ela é o núcleo de toda a hierarquia de protocolos. Sua função é promover uma transferência de dados confiável e econômica entre a máquina de origem e a máquina de destino, independente das redes físicas em uso no momento. Sem a camada de transporte, todo o conceito de protocolos em camadas faria pouco sentido.

O principal objetivo da camada de transporte é oferecer um serviço confiável, eficiente e econômico a seus usuários que, em geral, são processos presentes na camada de aplicação. Para atingir esse objetivo, a camada de transporte utiliza vários serviços oferecidos pela camada de rede. O hardware/software da camada de transporte que executa o trabalho é chamado entidade de transporte. A entidade de transporte pode estar localizada no núcleo do sistema operacional em um outro processo do usuário, em um pacote de biblioteca vinculado a aplicações de rede ou na placa de interface de rede.

10.4.1 - SERVIÇOS DE TRANSPORTE

Assim como existem dois tipos de serviço de rede, o serviço orientado a conexões e o serviço sem conexões, também existem dois tipos de serviço de transporte. O serviço de transporte orientado a conexões é semelhante ao serviço de rede orientado a conexões em muitos aspectos. Em ambos os casos, as conexões têm três fases: o estabelecimento, a transferência de dados e o encerramento. O endereçamento e o controle de fluxo também são semelhantes em ambas as camadas. Além disso, o serviço de transporte sem conexões é semelhante ao serviço de rede sem conexões.

10.4.2 - QUALIDADE DE SERVIÇO

A qualidade de serviço pode ser caracterizada por uma série de parâmetros QoS (Quality of Service):

- O retardo no estabelecimento da conexão.
- O retardo no encerramento da conexão.
- A probabilidade e de falha no estabelecimento da conexão.
- A probabilidade de falha na liberação da conexão.
- A vazão em cada sentido da conexão.
- O retardo de transferência médio, também em cada sentido.
- O retardo de transferência máximo, também em cada sentido.
- A variação estatística do retardo.
- A taxa de erro, expressa em porcentagem dos bits transmitidos.
- A prioridade, ou a garantia de que serviços de maior prioridade tenham preferência sobre os de mais baixa prioridade.
- Probabilidade de queda de uma conexão.

10.4.3 - AS PRIMITIVAS DA CAMADA DE TRANSPORTE

As primitivas da camada de transporte são as seguintes:

- LISTEN - coloca uma porta em modo de espera de conexões.
- CONNECT - estabelece uma conexão para uma porta.
- SEND - envia dados.
- RECEIVE - recebem dados.
- DISCONNECT - desconecta uma conexão ativa.

Para transmissões não orientadas a conexão, as chamadas CONNECT e DISCONNECT não são usadas. Todo dado transmitido pela camada de transporte é encapsulada nos formatos de pacotes das camadas inferiores.

As primitivas são as seguintes:

- **Socket -** cria um novo socket (sem um IP ou porta designada).
- **Bind** - atribui um endereço IP e uma porta para um socket.
- **Listen** - coloca um socket em modo de escuta e determina o tamanho da fila do socket para conexões não atendidas.
- **Accept** - bloqueia o programa até o socket receber uma conexão.
- **Connect -** estabelece uma conexão com um outro socket.
- **Send** - enviam dados através de um socket.
- **Receive** - recebem dados através de um socket.
- **Close/Shutdown -** encerra uma conexão.

10.4.4 - ELEMENTOS DA CAMADA DE TRANSPORTE

A camada de transporte se parece com a camada de enlace no aspecto de que ambas têm que gerenciar correção de erro, controle de fluxo entre outros aspectos.

Porém, uma série de diferenças existem entre ambas:

• A camada de enlace opera num link físico enquanto que a camada de transporte opera numa rede inteira.
• Na camada de enlace, não é necessário especificar qual roteador será acessado porque cada linha acessa diretamente o roteador. Na camada de transporte o endereço do roteador é necessário.
• O estabelecimento de conexões é mais simples na camada de enlace porque o "outro lado" está sempre disponível. Na camada de transporte é mais complicado.
• Outro fator complicado para a camada de transporte é o efeito de armazenamento da rede que não acontece na camada de enlace. Um pacote pode ser enviado por uma rede e obter uma rota diferente chegando ao destino muito tempo depois dos pacotes seguintes que foram enviados.
• Apesar das duas camadas necessitarem de buffers, controle de fluxo e erro, na camada de transporte o tratamento disso é bem mais complexo porque ela lida com várias conexões simultâneas, o que não ocorre na camada de enlace.

10.4.5 - MULTIPLEXAÇÃO[8]

Na camada de transporte como também em outras camadas da arquitetura de rede também há a necessidade da multiplexação. A multiplexação pode ser:

• A multiplexação ascendente, que é a multiplexação de várias conexões de transporte na mesma conexão de rede.
• A multiplexação descendente, onde a camada de transporte abre várias conexões de rede e distribui o tráfego por eles em rodízio.

10.4.6 - PROCOLO UDP

O conjunto de protocolos da internet admite um protocolo de transporte sem conexões, o UDP (User Datagram Protocol). O UDP oferece um meio para as aplicações enviarem datagramas IP encapsulados sem que seja necessário estabelecer uma conexão. O UDP é descrito na RFC 768. O UDP transmite segmentos que consistem em um cabeçalho de 8 bytes, seguido pela carga útil. Quando um pacote UDP chega, sua carga útil é entregue ao processo associado à porta de destino.

8 - Multiplexação é uma técnica que permite trafegar vários sinais de comunicação por um único meio de transmissão.

10.5 – EXERCÍCIO PROPOSTO

1 - Defina Camada Física da Rede.

_____
_____
_____

11 – CAMADA DE APLICAÇÃO

A camada de aplicação contém uma série de protocolos comumente necessários para os usuários. As camadas situadas abaixo da camada de aplicação têm a função de oferecer um serviço de transporte confiável, mas, na verdade, elas não executam qualquer tarefa para os usuários. Vamos conhecer alguns protocolos de suporte que são essenciais para que as aplicações funcionem.

11.1 - DNS – *DOMAIN NAME SYSTEM* – SISTEMA DE NOMES DE DOMÍNIOS

Quando você visita um site através do seu navegador ou quando envia um e-mail, a internet precisa saber em qual servidor o site e o e-mail estão armazenados para poder responder à sua solicitação. A informação da localização destes servidores está em um servidor chamado DNS *(Domain Name Server)*.

Cada domínio possui um registro no DNS que define qual o endereço IP do servidor de hospedagem e o IP do servidor de e-mail que responderão por este domínio. O processo para a descoberta dos servidores que respondem por um domínio é denominado resolução do nome ou resolução do domínio.

Os navegadores e os sistemas-clientes de e-mail solicitam que a internet faça a resolução do domínio para apresentar um site ou enviar um e-mail. Esse processo é totalmente transparente para o usuário, que apenas digita o site que quer visitar e o navegador descobre em qual servidor o site está hospedado e, em seguida solicita para o servidor de hospedagem que envie a página inicial.

Por segurança, um domínio pode definir vários servidores DNS. O DNS primário é o primeiro sistema a ser consultado no momento da resolução do nome, caso o servidor DNS primário esteja em manutenção, o servidor DNS secundário é consultado e, assim sucessivamente. O DNS é definido nas RFC´s 1034 e 1035.

Existem treze servidores DNS raiz no mundo todo e sem eles a internet não funcionaria. Destes, dez estão localizados nos Estados Unidos da América, um na Ásia e dois na Europa. Para aumentar a base instalada destes servidores, foram criadas réplicas localizadas por todo o mundo, inclusive no Brasil desde 2003. Ou seja, os servidores de diretórios responsáveis por prover informações como nomes e endereços das máquinas são normalmente chamados servidores de nomes. Na internet, os serviços de nomes usados é o DNS, que apresenta uma arquitetura cliente/servidor, podendo envolver vários servidores DNS na resposta a uma consulta.

11.2 HTTP - O QUE É?

O HTTP (*Hypertext Transfer Protocol ou Protocolo de Transferência de Hipertexto*) é um protocolo de comunicação (na camada de aplicação segundo o Modelo OSI) responsável pelo tratamento de pedidos e respostas entre cliente e servidor na World Wide Web. Ele surgiu da necessidade de distribuir informações pela internet e para que essa distribuição fosse possível foi necessário criar uma forma padronizada de comunicação entre os clientes e os servidores da Web e entendida por todos os computadores ligados à internet. Com isso, o protocolo HTTP passou a ser utilizado para a comunicação entre computadores na internet e a especificar como seriam realizadas as transações entre clientes e servidores, através do uso de regras básicas.

Normalmente, este protocolo utiliza a porta 80 e é usado para a comunicação de sites Web, comunicando na linguagem HTML. Contudo, para haver comunicação com o servidor do site é necessário utilizar comandos adequados, que não estão em linguagem HTML.

Este protocolo tem sido usado pela WWW desde 1990. A primeira versão de HTTP, chamada HTTP/0.9, era um protocolo simples para a transferência de dados no formato de texto ASCII pela internet, através de um único método de requisição, chamado GET. A versão HTTP/1.0 foi desenvolvida entre 1992 e 1996 para suprir a necessidade de transferir não apenas texto. Com essa versão, o protocolo passou a transferir mensagens do tipo MIME44 (Multipurpose Internet Mail Extension) e foram implementados novos métodos de requisição, chamados POST e HEAD.

No HTTP/1.1, versão atual do protocolo descrito na RFC 2616, foi desenvolvido um conjunto de implementações adicionais ao HTTP/1.0, como por exemplo: o uso de conexões persistentes; o uso de servidores proxy que permitem uma melhor organização da cache; novos métodos de requisições; entre outros.

11.2.1 – FUNCIONAMENTO

Um sistema de comunicação em rede possui diversos protocolos que trabalham em conjunto para o fornecimento de serviços. Para que o protocolo HTTP consiga transferir seus dados pela Web, é necessário que os protocolos TCP e IP (Internet Protocol - Protocolo de Internet) tornem possível a conexão entre clientes e servidores através de sockets TCP/IP.

O HTTP utiliza o modelo cliente-servidor, como a maioria dos protocolos de rede, baseando-se no paradigma de requisição e resposta. Um programa requisitante (cliente) estabelece uma conexão com um outro programa receptor (servidor) e envia-lhe uma requisição, contendo a URL, a versão do protocolo, uma mensagem MIME (padrão utilizado para codificar dados em formato de textos ASCII para serem transmitidos pela internet) contendo os modificadores da requisição, informações sobre o cliente e, possivelmente, o conteúdo no corpo da mensagem.

O servidor responde com uma linha de status (status line) incluindo sua versão de protocolo e um código de operação bem sucedido ou um código de erro, seguido pelas informações do servidor, meta, informações da entidade e possível conteúdo no corpo da mensagem. Após o envio da resposta pelo servidor, encerra-se a conexão estabelecida.

11.3 - FTP - O QUE É?

O FTP (*File Transfer Protocol ou Protocolo de Transferência de Arquivos*) é uma forma bastante rápida e versátil de transferir arquivos (também conhecidos como ficheiros), sendo uma das mais usadas na internet.

A transferência de dados em redes de computadores envolve normalmente transferência de arquivos e acesso a sistemas de arquivos remotos (com a mesma interface usada nos arquivos locais). O FTP (RFC 959) é baseado no TCP, mas é anterior a pilha de protocolos TCP/IP, sendo posteriormente adaptado para o TCP/IP. É o padrão da pilha TCP/IP para transferir arquivos, é um protocolo genérico independente de hardware e do sistema operacional e transfere arquivos por livre-arbítrio, tendo em conta restrições de acesso e propriedades dos mesmos.

11.3.1 – FUNCIONAMENTO

A transferência de arquivos se dá entre um computador chamado "cliente" (aquele que solicita a conexão para a transferência de dados) e um servidor (aquele que recebe a solicitação de transferência). O cliente, através de software específico, pode selecionar quais arquivos enviar ou receber do servidor. Para existir uma conexão ao servidor, caso o servidor exija, o utilizador informa um nome de utilizador (nome de usuário) e uma senha, bem como o nome correto do servidor ou seu endereço IP, seria uma conexão de controle para a sessão. Se os dados foram informados corretamente, a conexão pode ser estabelecida, utilizando-se dois canais de comunicação, chamados de portas (ports),

a primeira será realizada pelo cliente que realiza uma conexão TCP para a porta 21 do servidor. Essa conexão, chamada de conexão de controle, permanece aberta ao longo da sessão enquanto uma segunda conexão, chamada conexão de dados, é estabelecida na porta 20 do servidor e em alguma porta do cliente, quando requisitado para a transferência de arquivo.

Uma transferência de arquivo em progresso, sobre uma conexão de dados, pode ser abortada utilizando uma mensagem de interrupção enviada sobre a conexão de controle. FTP pode ser executado em modo ativo ou passivo, os quais determinam como a conexão de dados é estabelecida. No modo ativo, o cliente envia para o servidor o endereço IP e o número da porta na qual ele irá ouvir e, então o servidor inicia a conexão TCP. Em situações onde o cliente está atrás de um firewall e inapto para aceitar entradas de conexões TCP, o modo passivo pode ser utilizado. A transferência de dados pode ser feita em qualquer um dos três modos a seguir:

a) **Modo Fluxo** – o dado é enviado como um fluxo contínuo, liberando FTP de fazer algum processamento. Ao invés disso, todo processamento é deixado para o TCP. Nenhum indicador de fim de arquivo é necessário, a menos que o dado esteja dividido dentro de registros.
b) **Modo de Bloqueio** - FTP quebra o dado dentro de vários blocos (bloco de cabeçalho, contagem de byte e campo de dado) e então o passa para o TCP.
c) **Modo Comprimido** - dado é comprimido utilizando um algoritmo simples.

11.4 - SMTP - O QUE É?

O SMTP (Simple Mail Transfer Protocol ou Protocolo de Transferência de E-mail Simples) é o protocolo padrão para envio de e-mails através da internet. É um protocolo relativamente simples, baseado em texto simples, onde um ou vários destinatários de uma mensagem são especificados (na maioria dos casos, validados) sendo, depois, a mensagem transferida. Para envio de e-mail é bastante fácil testar um servidor SMTP usando o programa Telnet.

11.4.1 - FUNCIONAMENTO

Esse protocolo roda sobre a porta 25 numa rede TCP. A resolução DNS de um servidor SMTP de um dado domínio é possibilitada por sua entrada MX (Mail eXchange).

O Sendmail foi um dos primeiros (se não o primeiro) agente de transporte de e-mail a implementar SMTP. Dada a especificação inicial, que contemplava apenas texto ASCII, este protocolo não é ideal para a transferência de arquivos (também chamados de ficheiros). Alguns standards foram desenvolvidos para permitir a transferência de ficheiros em formato binário através de texto simples, como o caso do MIME. Hoje em dia quase todos os servidores SMTP suportam a extensão 8BITMIME.

O SMTP é um protocolo de envio apenas, o que significa que ele não permite que um usuário descarregue as mensagens de um servidor. Para isso, é necessário um cliente de e-mail com suporte ao protocolo POP3 ou IMAP, que é o caso da maioria dos clientes atuais.

11.5 - POP - O QUE É?

O Post Office Protocol (POP3) é um protocolo utilizado no acesso remoto a uma caixa de correio eletrônico. Ele permite que todas as mensagens contidas numa caixa de correio eletrônico possam ser transferidas sequencialmente para um computador local. Aí, o utilizador pode ler as mensagens recebidas, apagá-las, responder-lhes, armazená-las e etc.

11.5.1 – FUNCIONAMENTO

O funcionamento do protocolo POP3 diz-se off-line, uma vez que é o processo suportado

se baseia nas seguintes etapas:

- É estabelecida uma ligação TCP entre a aplicação cliente de e-mail e o servidor onde está a caixa de correio (servidor de e-mail). O cliente autentica-se e todas as mensagens existentes na caixa de correio são transferidas sequencialmente para o computador local. As mensagens são apagadas da caixa de correio (opcionalmente, o protocolo pode ser configurado para que as mensagens não sejam apagadas da caixa de correio). A ligação com o servidor é terminada. O utilizador pode agora ler e processar as suas mensagens (off-line).

A característica off-line do protocolo POP3 é útil para utilizadores que se ligam à internet através de redes com banda baixa ou limitada. Com o POP3, a ligação apenas precisa estar ativa durante a transferência das mensagens, e a leitura e processamento das mensagens pode depois ser efetuada com a ligação inativa.

11.6 – EXERCÍCIO PROPOSTO

1 - Defina DNS.

_____
_____
_____

12 - SEGURANÇA DE REDES

Começamos esse assunto sobre segurança afirmando como fez Wadlow em seu livro que segurança não é uma tecnologia, não é possível uma empresa fornecer um software capaz de proteger completamente um computador. "Segurança é a direção em que se pode viajar, mas nunca chegando de fato ao destino" o importante é conhecer e administrar, para alcançar um nível aceitável de segurança.

WADLOW, p.4 diz: "*A segurança é um processo*". Pode-se aplicar o processo seguidamente à rede e à empresa que a mentem e, dessa maneira, melhorar a segurança dos sistemas. Se não iniciar ou interromper a aplicação do processo sua segurança será cada vez pior, à medida que surgirem novas ameaças técnicas.

12.1 – SEGURANÇA DA INFORMAÇÃO NAS REDES

A informação é um ativo muito importante, tanto para empresa, como para indivíduos. Evidente que não nos referimos a qualquer informação, mas àquela que movimenta o ambiente de negócios.

Segundo CARUSO, 1999, p. 21, "*Ao longo da história, o ser humano sempre buscou o controle sobre as informações, que lhes eram importantes de alguma forma; isso é verdadeiro mesmo na mais remota antiguidade*".

A norma ABNT NBR ISO/IEC 17799:2005 diz: "*Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio"*. Com o avanço da tecnologia, esta informação ficou exposta a ameaças. A Segurança da Informação envolve aspectos de proteção e implementação de políticas adequadas, procedimentos em software, hardware e pessoal, objetivando reduzir pontos fracos e garantir segurança aos mesmos. Em software, podemos mencionar proteção contra vírus, backdoors[9] , worms[10] , spywares[11] e exploits[12] . Em hardware, existe a necessidade de segurança física, do local, acondicionamento do ambiente e das pessoas. Destacamos a implantação de políticas de logons e senhas seguras e procedimentos de conscientização, educação e treinamento em segurança, evitando a prática de engenharia social e a utilização incorreta dos sistemas. A abordagem do tema segurança envolve instalação de firewall de rede, hardening[13] de servidores, antivírus corporativos, verificadores de integridade e sistemas de detecção de intrusos (IDS) que procuram antecipar possíveis tentativas de detecção de padrões.

---

9 - O backdoor se caracteriza pelo vírus que contamina a máquina através de um programa e a deixa exposta para uma futura invasão do cracker por acesso remoto.
10 - Um worm, assim como um vírus, cria cópias de si mesmo de um computador para outro, mas faz isso automaticamente.
11 - Spyware é o termo usado para descrever software que executa determinados comportamentos, como publicidade, recolha de informações pessoais ou alteração da configuração do computador, normalmente sem o seu consentimento prévio.
12 - Exploits na verdade pode ser um programa executável ou um código ainda não compilado, eles são criados por hackers, crackers ou simplesmente programadores para explorar sistemas, programas e sites vulneráveis.
13 - Hardening (fortalecimento) é um processo de mapeamento das ameaças, mitigação dos riscos e execução das atividades corretivas - com foco na infraestrutura e objetivo principal de torná-la preparada para enfrentar tentativas de ataque.

12.2 – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A implementação de políticas de segurança visa estabelecer normas para encontrar vulnerabilidades que podem ser exploradas e violadas. Políticas de implementação de segurança correspondem a um conjunto de procedimentos que estabelecem limites à utilização dos sistemas pelos usuários, controle de acesso e autenticação, aplicando os conceitos básicos da segurança da informação: confidencialidade, integridade e disponibilidade. Por confidencialidade entende-se que somente o remetente e o destinatário pretendido, devem poder entender o conteúdo da mensagem. Na integridade, o conteúdo não deve ser alterado, por acidente ou má intenção durante a transmissão; na autenticação é importante que seja confirmado a identidade da outra pessoa, ou seja, confirmar que é ele mesmo quem diz ser e por fim; na disponibilidade é fundamental que a comunicação esteja sempre à disposição dos envolvidos.

Em Crime by Computer, o autor Donn B. Parker cita o primeiro caso de violação de segurança em T.I. – Tecnologia da Informação - que se teve notícia nos EUA, mais precisamente no Estado de Minnesota, noticiado através do Minneapolis Tribune, no dia 18 de outubro de 1966, sob o título "PERITO EM COMPUTADOR ACUSADO DE FALSIFICAR SEU SALDO BANCÁRIO".

12.3 – INCIDENTES DE SEGURANÇA

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, Cert.br, é um grupo de respostas a incidentes de segurança para internet no Brasil. Nem todas as empresas reportam ao Cert.br as vulnerabilidades que foram submetidas. Pelos gráficos obtidos vemos claramente o crescimento de ataques as redes. Tal crescimento indica a necessidade das empresas desenvolverem novas técnicas de combate ao crime informático.

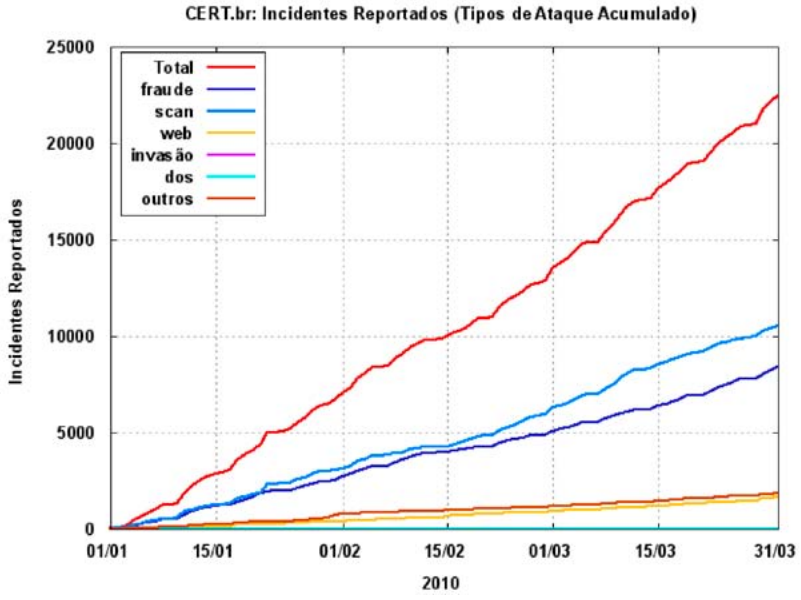


Imagem 26

A figura 1 apresenta o total de incidentes reportados ao CERT, de janeiro a março de 2010. As invasões ocorrem por motivos diversos através de procedimentos que possuem o intuito de obter informações confidenciais, utilizar recursos do sistema, lucrar, praticar o vandalismo (defacement[14]), por vingança pessoal ou até mesmo curiosidade.

14 - Defacement (ou simplesmente deface) é um termo de origem inglesa para o ato de modificar ou danificar a superfície ou aparência de algum objeto e, é empregado comumente na Segurança da Informação para categorizar os ataques realizados por defacers e script kiddies para modificar a página de um sítio na internet.

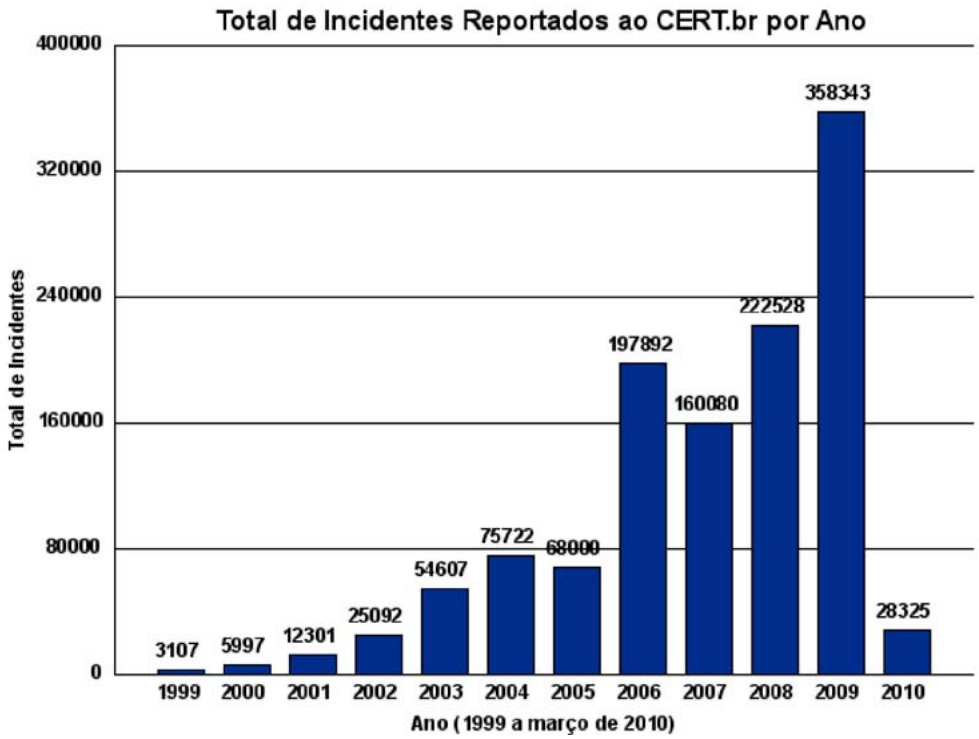


Imagem 27

Na figura 2 observamos o crescimento de incidentes reportados ao Cert.br[15] no ano de 2009. Uma das dificuldades encontradas pelo Cert.br é que muitas empresas não notificam os incidentes sofridos, portanto, os números citados são das empresas que reportam as informações e não da totalidade de incidentes causados no Brasil.

12.4 - TÉCNICAS DE SEGURANÇA DA INFORMAÇÃO

Para conhecimento, destacamos mecanismos que podem e devem ser utilizados como acessórios que contemplam a segurança da informação. Salientamos, no entanto, que nenhum sistema é 100 % seguro e que as políticas de segurança trazem à empresa a formação de um ambiente físico e logicamente seguro. Não é propósito desse trabalho, detalhar cada item, e sim, indicar algumas ferramentas para utilização no ambiente informatizado: atualizações de segurança do sistema operacional que corrigem as vulnerabilidades, antivírus, firewalls, criptografia[16] , detecção de intrusos (IDS)[17] e testes de negação de serviços (DoS)[18] , plano de contingência, recuperação de informação e softwares de administração de redes. Segundo (CARUSO,1999) "De nada adianta dispor de um sistema completo e que garante a sobrevivência dos meios de armazenamento se não adotam procedimentos operacionais destinados a garantir a segurança dos mesmos."

15 - CERT.br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil - é o Grupo de Resposta a Incidentes de Segurança para a Internet Brasileira, mantido pelo Comitê Gestor da Internet no Brasil. É o grupo responsável por receber, analisar e responder a incidentes de segurança em computadores, envolvendo redes conectadas à internet brasileira.
16 - Criptografia é o ato de codificar dados em informações aparentemente sem sentido, para que pessoas não consigam ter acesso às informações que foram cifradas.
17 - Sistema de Detecção de Intrusos (IDS).
18 - Negação de Serviços (DoS) - Tipo de Ataque muito comum na internet, desligam serviços, servidores.

12.5 – REQUISITOS DE SEGURANÇA

Para entendermos os tipos de ameaças à segurança que existem. A segurança de computador e da rede trata de quatro requisitos.

12.5.1 - PRIVACIDADE

Exige que todos os dados sejam acessíveis apenas a pessoas autorizadas. Isso envolve qualquer forma de exposição de dados.

12.5.2 - INTEGRIDADE

Exige que apenas pessoas autorizadas possam modificar dados.

12.5.3 - DISPONIBILIDADE

Exige que todos os dados estejam disponíveis as pessoas autorizadas.

12.5.4 - AUTENTICIDADE

Exige que um host ou serviço seja capaz de verificar a identidade de um usuário.

12.6 - EXECÍCIO PROPOSTO

1 - O que é Backdoor?

_____
_____
_____

13 - ADMINISTRAÇÃO E OPERAÇÃO SEGURA DE REDES E SISTEMAS

13.1 - EDUCAÇÃO DOS USUÁRIOS

Uma tarefa extremamente importante e que deve fazer parte do cotidiano de administradores de redes é a constante educação dos usuários. Sabe-se que grande parte dos problemas de segurança são originados na rede interna da organização e, muitas vezes, são causados pelo desconhecimento de conceitos e procedimentos básicos de segurança por parte dos usuários.

Um exemplo clássico deste problema é a má configuração do programa de leitura de e-mails de um usuário, que faz com que qualquer arquivo anexado a uma mensagem seja automaticamente aberto ou executado, permitindo a instalação de backdoors, cavalos de troia, disseminação de vírus e etc.

O primeiro fator que contribui diretamente para o processo de educação é o estabelecimento de políticas de segurança e de uso aceitável, claro, sem ambiguidade, conhecido e completamente entendido pelos usuários da rede.

Outro fator importante é o estabelecimento de um canal de comunicação, por exemplo, através de listas de e-mails, onde informações sobre questões relevantes de segurança são frequentemente passadas para os usuários da rede. A descoberta de uma vulnerabilidade de segurança que afeta o servidor Web da organização podendo não ser relevante para os usuários, mas a notificação da descoberta de um novo vírus, sua forma de infecção e métodos de prevenção são informações que devem ser conhecidas e aplicadas por todos os usuários.

Muitas vezes e, principalmente, em grandes organizações, tarefas como a instalação e configuração do sistema operacional e softwares de um computador são realizadas pelo próprio usuário. Daí vem um dos fatores de grande importância neste processo de educação, pois a execução de tais tarefas têm impacto direto na segurança das redes e sistemas de uma organização.

Procurando cobrir os tópicos necessários para a educação do usuário, dentre outras questões, foi desenvolvida a "Cartilha de Segurança para a Internet", que tem por finalidade sanar algumas dúvidas comuns sobre segurança de computadores e redes e, sobre o significado de termos e conceitos amplamente utilizados na internet. Além disso, a cartilha procura enumerar, explicar e fornecer um guia para uma série de procedimentos que visam aumentar a segurança de um computador e de posturas que um usuário pode adotar para garantir sua segurança na internet. Este documento pode ser obtido em http://cartilha.cert.br/.

13.2 - AJUSTE DO RELÓGIO

13.2.1 - SINCRONIZAÇÃO DE RELÓGIOS

Os relógios de todos os sistemas da sua rede (incluindo as estações de trabalho) deverão estar sincronizados, ou seja, deverão ter exatamente o mesmo horário. Para que isso aconteça, você deve usar um protocolo de sincronização de relógios, tal como o NTP (*Network Time Protocol*). Este protocolo é o mais recomendado, pois existem implementações dele para os mais variados sistemas operacionais, como pode ser visto em: http://www.ntp.org/.

Para obter maior precisão no ajuste e para minimizar o tráfego desnecessário na rede,

sugere-se que a sincronização via NTP seja implementada observando-se as seguintes recomendações:

☐ Procure manter em sua rede um servidor NTP local. Esse servidor é quem irá realizar a sincronização com um servidor externo. As demais máquinas da sua rede, por sua vez, terão seus relógios sincronizados com o relógio do servidor local.
☐ Muitos *backbones* disponibilizam um servidor NTP a seus clientes. Consulte o suporte técnico do seu *backbone* para verificar se ele oferece este serviço e como você pode fazer para utilizá-lo.

13.2.2 - TIMEZONE

Caso você trabalhe com servidores Unix, ajuste o relógio de hardware destes sistemas para a hora padrão de Greenwich (GMT) e configure adequadamente o seu fuso horário (*timezone*) para que a hora local seja exibida corretamente. O uso do *timezone* certo também possibilita o ajuste automatizado do relógio por conta do horário de verão. Para que isso seja possível, você deverá criar ou obter um arquivo de informações de *timezone* com as datas corretas de início e fim do horário de verão. Para maiores informações, consulte a documentação do comando zic.

13.3 - EQUIPES DE ADMINISTRADORES

Em muitas redes, a administração de sistemas é uma responsabilidade dividida entre várias pessoas. Nesses casos, é necessário estabelecer algumas regras para garantir a eficiência do trabalho em equipe.

13.3.1 - COMUNICAÇÃO EFICIENTE

Em primeiro lugar, é essencial que os diferentes administradores comuniquem-se de maneira eficiente. Um bom modo de fazer isto é estabelecer listas de discussão por e-mail que sejam internas a sua organização. Estas listas podem ser usadas para, entre outros propósitos, comunicar alterações na configuração dos sistemas, notificar os demais administradores a respeito de ocorrências relevantes e servir como mecanismo de acompanhamento da divisão de tarefas.

A grande vantagem de usar listas de discussão é que elas possibilitam a comunicação entre os administradores mesmo que alguns trabalhem em diferentes turnos ou locais. O histórico das listas pode servir para documentar decisões tomadas e, para atualizar um administrador que tenha passado algum tempo afastado de suas atividades.

13.3.2 - CONTROLE DE ALTERAÇÕES NA CONFIGURAÇÃO

A partir do momento em que várias pessoas ficam encarregadas da administração de um sistema, torna-se necessário dispor de meios que possibilitem a identificação de quem foi o responsável por cada alteração na sua configuração. Isso permite resolver problemas de forma mais eficiente, pois a pessoa que realizou determinada modificação é a mais indicada para ajudar na resolução de eventuais complicações dela decorrentes.

Conforme mostrado na seção 3.3, o logbook pode auxiliar nessa tarefa. Para isso, é necessário que em cada entrada no logbook conste o nome da pessoa responsável pelas modificações ali descritas.

Uma forma mais automatizada de fazer isso é através do uso de ferramentas de controle de versão como o RCS (http://www.cs.purdue.edu/homes/trinkle/RCS/) e o CVS (http://www.cvshome.org). Essas ferramentas também permitem manter um histórico de arquivos de configuração, de forma a possibilitar a recuperação de antigas versões desses arquivos.

Recomenda-se que, sempre que possível, este tipo de ferramenta seja usado em sistemas que possuam múltiplos administradores.

13.3.3 - USO DE CONTAS PRIVILEGIADAS

Um problema que surge em sistemas com múltiplos administradores é a dificuldade de se manter um registro do uso de contas privilegiadas, tais como root e Administrator.
Sempre que possível, estas contas não devem ser usadas diretamente. Um administrador deve entrar no sistema usando sua conta pessoal e a partir dela realizar suas tarefas, usando os privilégios mais elevados apenas quando estritamente necessário. Em sistemas Unix, isso é realizado através do comando su. O su traz como benefício adicional o fato de que o seu uso normalmente fica registrado nos logs do sistema, permitindo que se identifique quem acessou a conta de root em um determinado período.

O sudo (http://www.courtesan.com/sudo/) é uma ferramenta que permite que o administrador do sistema conceda a determinados usuários a possibilidade de executar comandos predefinidos como se eles fossem root (ou outro usuário), registrando nos logs do sistema a utilização desses comandos. O uso do sudo reduz a necessidade de compartilhamento da senha de root, uma vez que os usuários entram com sua própria senha para utilizar os comandos disponíveis através dele. Isso pode ser usado, por exemplo, quando existem contas de operador que são usadas para a realização de backups ou para invocar o procedimento de desligamento do sistema.

O sudo é extremamente configurável, possibilitando, entre outros recursos, a definição de grupos de usuários, de comandos e de hosts e o uso de restrições por host ou grupo de hosts (permitindo que o mesmo arquivo de configuração seja usado em sistemas diferentes).

IMPORTANTE --> O uso de uma conta administrativa única com senha compartilhada, que não permita determinar qual dos administradores acessou o sistema, deve ser evitado ao máximo.

13.4 - LOGS

Logs são muito importantes para a administração segura de sistemas, pois registram informações sobre o seu funcionamento e sobre eventos por eles detectados. Muitas vezes, os logs são o único recurso que um administrador possui para descobrir as causas de um problema ou comportamento anômalo.

13.4.1 - GERAÇÃO DE LOGS

Para que os logs de um sistema sejam úteis para um administrador, eles devem estar com o horário sincronizado via NTP, ser tão detalhado quanto possível, sem, no entanto gerar dados em excesso. Informações especialmente úteis são aquelas relacionadas a eventos de rede, tais como conexões externas e registros de utilização de serviços (arquivos transferidos via FTP, acessos a páginas Web, tentativas de login sem sucesso, avisos de disco cheio e etc.).

Para registrar estas informações, é necessário configurar o sistema da maneira apropriada. A forma de fazer isto geralmente varia para cada componente específico; consulte a documentação para descobrir como habilitar o logging de informações no seu sistema e em softwares específicos como firewalls e servidores HTTP.

13.4.2 - ARMAZENAMENTO DE LOGS

- **Armazenamento on-line**

Os logs são tradicionalmente armazenados em disco, no próprio sistema onde são gerados. Essa é a opção mais óbvia, mas ela possui alguns riscos inerentes que devem ser

compreendidos. O primeiro deles diz respeito à possibilidade dos logs serem destruídos durante uma invasão do sistema (uma ocorrência bastante comum). Em alguns sistemas, isso pode ser contornado através da instalação de um loghost centralizado. Um loghost centralizado é um sistema dedicado à coleta e ao armazenamento de logs de outros sistemas em uma rede, servindo como um repositório redundante de logs. Via de regra, o loghost não disponibiliza nenhum outro serviço, nem mesmo acesso remoto para os administradores, para minimizar a possibilidade de que ele seja comprometido. Outra vantagem de loghosts centralizados é que eles facilitam a análise dos logs e correlação de eventos ocorridos em sistemas distintos. Sempre que possível, o uso de loghosts centralizados é fortemente recomendado.

Um segundo risco é a possibilidade de um atacante usar o logging para executar um ataque de negação de serviço contra um determinado sistema, gerando eventos em excesso até que o disco onde são armazenados os logs fique cheio e o sistema trave em consequência disto. Conforme discutido na seção 3.2, o uso de uma partição separada para armazenar os logs pode minimizar o impacto deste problema.

Outro ponto que merece atenção é a rotação automática de logs. Quando este recurso é utilizado, deve-se garantir que os logs sejam movidos para o armazenamento off-line antes que eles sejam removidos do sistema pela rotação, evitando assim a perda de registros. Alguns sistemas trazem a rotação automática habilitada na sua configuração padrão; ao instalar um destes sistemas, verifique se esta configuração é compatível com os seus procedimentos de backup e armazenamento off-line de logs.

13.5 - CUIDADOS COM REDES RESERVADAS

Existem alguns blocos de endereços IP que são reservados pelo IANA (*Internet Assigned Numbers Authority*) para propósitos específicos. Não existe um documento único que registre todos estes blocos; alguns estão documentados em RFC´s, enquanto que outros são considerados reservados por razões de compatibilidade histórica.

A RFC 33306 lista vários blocos reservados pelo IANA. Uma lista dessas redes reservadas conhecidas é mostrada na tabela 1, juntamente com um breve comentário sobre a finalidade de cada rede.

Tabela 1: Lista de redes reservadas pelo IANA

REDE	COMENTÁRIO
0.0.0.0/8	Usada por sistemas antigos para Broadcast.
127.0.0.0/8	Loopback.
192.0.2.0/24	TEST-NET; usada para exemplos em documentação.
10.0.0.0/8	Usada em redes privadas (RFC 1918).
172.16.0.0/12	Usada em redes privadas (RFC 1918).
192.168.0.0/16	Usada em redes privadas (RFC 1918).
169.254.0.0/16	Usada para autoconfiguração (está relacionada ao protocolo DHCP).
192.88.99.0/24	Usada para 6to4 Relay Anycast (RFC 3068).
198.18.0.0/15	Usada para testes de desempenho de equipamentos de rede (RFC 2544).
240.0.0.0/4	Classe D
240.0.0.0/5	Classe E

Outro ponto importante é que nem todo o espaço de endereçamento IPv4 está atualmente alocado. Uma lista dessas redes não alocadas, e portanto, reservadas para o IANA, é mantida em http://www.iana.org/assignments/ipv4-address-space. Esta lista é frequentemente atualizada e é recomendável que seja consultada regularmente. Endereços não alocados

e pertencentes a blocos reservados não devem ser propagados através da internet, sendo recomendada a sua filtragem no perímetro da sua rede, tanto para entrada quanto para saída.

Caso você possua redes privadas com IP´s reservados, certifique-se de que os endereços utilizados sejam os especificados na RFC 19187 (10.0.0.0/8, 172.16.0.0/12 e 192.168.0.0/16). Endereços reservados não devem estar associados a nomes em servidores DNS públicos.

Se você utilizá-los em redes privadas e quiser usar nomes para as máquinas, configure um servidor DNS privado ou utilize tabelas de hosts (/etc/hosts ou C:\WINDOWS\HOSTS). Caso você detecte um ataque proveniente de uma das redes da tabela 1 e estes endereços estiverem sendo filtrados no perímetro, os pacotes correspondentes só podem ter partido de dentro da sua própria rede. A causa mais frequente para isso é a existência de erros de configuração que fazem com que os endereços reservados "vazem" de uma ou mais de suas redes privadas. Logo, deve-se procurar internamente a causa do problema em vez de tentar contatar o IANA (que é a entidade listada nos contatos de WHOIS para estes blocos).

13.6 – EXERCÍCIO PROPOSTO

1 - O que são Log´s?

_____
_____
_____

14 – FIREWALL

Firewall "parede de fogo" é o nome dado ao dispositivo de rede, que tem por função, regular o tráfego de rede entre redes distintas e impedir a transmissão de dados nocivos ou não autorizados de uma rede a outra, separa sua intranet do mundo exterior, mas também, um *firewall* pode ser usado eficientemente numa intranet que não chega a ter acesso à internet.

Um *firewall* pode ajudar a impedir que hackers ou softwares mal-intencionados (como worms) obtenham acesso ao seu computador através de uma rede ou da internet. Um *firewall* também pode ajudar a impedir o computador de enviar software mal-intencionado para outros computadores.

No decorrer dos anos a internet já sofreu várias mudanças. A principal dela é a banda larga ao invés da discada, além disso ela está cada vez mais rápida, potente, de fácil integração, comunicação, troca de informação e multitarefa.

Da mesma forma que várias vantagens aos usuários surgiram, na mesma proporção apareceram as ameaças virtuais. Vírus cada vez mais potente, ataque de hackers, roubo de informações entre outras tantas ameaças. A partir de tantos perigos em potencial a internet precisou ser assegurada de tais ataques. Para isso, existem diversos programas que prometem defender o sistema e mantê-lo em pleno funcionamento. Umas das técnicas mais utilizadas é o que conhecemos por *firewall*.

Da mesma forma que você não deseja que pessoas invadam sua privacidade, roubem sua casa, é necessário trancar as portas e janelas. O *firewall* possui praticamente a mesma função, ele tranca as portas e janelas de seu computador. O *firewall* controla todos os dados transferidos de seu computador através da internet. Ele também é responsável pela prevenção de vazamento das informações do seu computador para a internet, desse modo, bloqueando o acesso de softwares que possam prejudicar o computador.

14.1 - FINALIDADE DO FIREWALL

O *firewall* serve como barreira de comunicação entre redes. Ele pode ser instalado em um roteador, computador ou conjunto de computadores que são especialmente configurados para "vigiar" os pacotes destinados à rede privada. Ele age de forma transparente para o usuário, isto é, o usuário não tem percebe que há um firewall.

A implementação de um *firewall* objetiva definir uma política de acesso à rede obrigando todos os pacotes direcionados à rede passem antes pelo *firewall*. Tomamos por exemplo, que a empresa estabeleça uma política de acesso que nenhum usuário dos computadores da empresa possa acessar o Facebook. A política de acesso é expressa através de regras. O *firewall* examina os pacotes, compara com as regras e bloqueia os pacotes suspeitos e/ou não autorizados.

14.2 - TIPOS DE FIREWALL

Existem diferentes tipos de *firewall*, que se distinguem pela forma como eles operam e os elementos que usam. Vamos conhecer alguns tipos bem conhecidos de firewall e sua operacionalização

14.2.1 - FILTROS INTELIGENTES

Os filtros inteligentes são aplicações executadas em computadores ligados ao roteador e

à rede interna. O tráfego de um lado para outro pode dar-se (ou não) conforme as regras estabelecidas nas aplicações. Em geral essa estratégia requer um equipamento extra, mas traz uma série de vantagens sobre os filtros baseados em roteador, principalmente em relação à monitoração de acesso:

- Roteadores, quando possuem algum tipo de log, não guardam informações muito precisas sobre as tentativas de conexão. Já os filtros inteligentes possuem vários níveis de logs, que facilitam identificar tentativas de acesso e até definir ações caso um evento relacionado à segurança ocorra.

14.2.2 - OS SERVIDORES PROXY

- Nesse tipo de *firewall* há um gateway (computador que faz uma ligação) entre o a rede interna e a internet. Ou seja, o gateway possui uma ligação com a rede externa e outra com a rede interna. Tudo que passa de uma para outra deve, obrigatoriamente, passar pelo gateway. O fato de terem duas ligações é que o faz ser chamado de "gateway de base dupla".
- Por exemplo, se José quer acessar um servidor de FTP em uma rede que possua este gateway de base dupla, primeiro Jose deve se conectar ao proxy (gateway), e a partir dele se conectar ao servidor FTP.
- Apontamos como vantagem desse tipo de *firewall* é o fato de esconder a estrutura interna da rede. Se João quiser acessar um serviço da rede, ele precisa apenas saber o IP do proxy e direcionar o pedido a ele. O proxy encaminha o pedido para o servidor apropriado.

14.3 - UM EXEMPLO DE FIREWALL: IPTABLES

O *IPTables* (ou *Netfilter)* é um *firewall* comum no Linux, que atua em nível de pacotes e funciona baseado no endereço/porta de origem/destino do pacote. O *IPTables* usa os seguintes conceitos:

a) **Regras** - são os comandos passados ao *IPTables* para realizar uma determinada ação de acordo com o endereço porta de origem/destino, interface de origem/destino etc. O *IPTables* usa a comparação dessas regras para a autorização ou não de um pacote que circula na rede.
b) **Chains** - as regras são armazenadas dentro dos *chains*, que podem ser de dois tipos: os embutidos (INPUT, OUTPUT e FORWARD) e os criados pelo usuário.
c) **Tabelas** - são locais usados para armazenar os *chains* e regras com características semelhantes. Existem três tabelas disponíveis no *IPTables*, que são FILTER, NAT e MANGLE. A tabela FILTER é a tabela padrão do *IPTables*. Nela são definidos quais pacotes podem passar e quais são rejeitados. Isso é justamente um filtro de pacotes. A tabela NAT *(Network Address Translation*) refere-se aos pacotes que vão sofrer tradução de endereço. A tabela MANGLE define quais pacotes serão modificados.
d) **Alvo** - é a ação a ser tomada quando um pacote chega ao final da *chain*. No *IPTables* existe: ACCEPT, DROP, REJECT e QUEUE. O ACCEPT permite ao pacote chegar ao seu destino. A ação DROP nega o pacote sem retornar mensagem. A ação REJECT nega a entrada do pacote retornando uma mensagem. O QUEUE envia pacote ao espaço do usuário.

O *IPTables* possuem vários comandos para manipular as *chains.* Por exemplo, -L[Chain] lista as regras de uma *chain.* Esse curso tem como finalidade dar uma visão geral de *firewall* e estamos citando o *IPTables* apenas para ilustrar. Não vamos detalhar a vasta lista de comandos disponibilizados pelo *IPTables*.

14.4 - FIREWALL É TOTALMENTE SEGURO?

O *firewall* não possui total segurança, pois a cada dia surgem mais pessoas interessadas em burlar o índice de segurança. Os hackers estão cada vez mais eficientes e oportunistas, a cada momento encontram novas maneiras de ultrapassar as barreiras de segurança

do *firewall* deixando que as informações do seu computador sejam compartilhadas e até espalhadas pelo mundo virtual. Vamos entender o seguinte: Se você tiver um *firewall* por software e porventura executar um programa obscuro que baixou de algum site da internet, esse mesmo programa é capaz de realizar uma nova configuração em seu *firewall* e desse momento em diante aceitar novas conexões obscuras. O firewall por hardware, por sua vez, mesmo que seu computador já esteja contaminado, o mesmo não é possível.

Exemplo de *firewall*

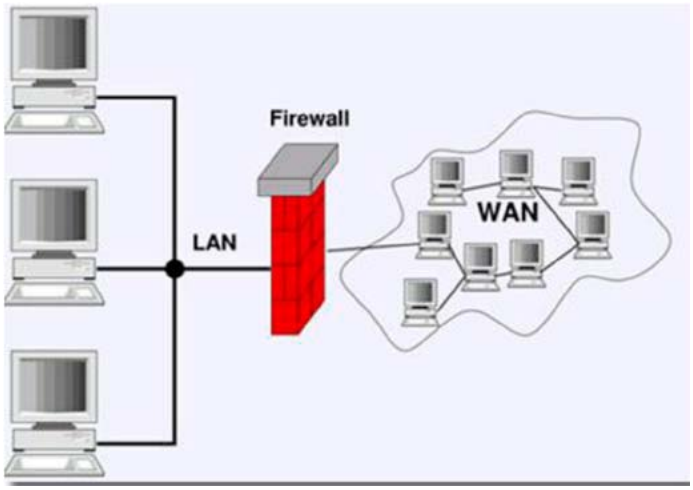


Imagem 28

14.5 - EXERCÍCIO PROPOSTO

1 - O que é Firewall?

_____
_____
_____

15 - CONCEITO DE CABEAMENTO - NORMAS DE CABEAMENTO

15.1 - HISTÓRIA

O primeiro experimento conhecido de conexão de computadores em rede foi feito em 1965, nos Estados Unidos, por obra de dois cientistas: Lawrence Roberts e Thomas Merril. A experiência foi realizada por meio de uma linha telefônica discada de baixa velocidade, fazendo a conexão entre dois centros de pesquisa em Massachusetts e na Califórnia. Estava plantada ali a semente para o que hoje é a internet – mãe de todas as redes.

O nascimento das redes de computadores, não por acaso, esta associada à corrida espacial. Boa parte dos elementos e aplicações essenciais para a comunicação entre computadores, como o protocolo TCP/IP, a tecnologia de comutação de pacotes de dados e o correio eletrônico, estão relacionados ao desenvolvimento da ARPANET, a rede que deu origem a internet. Ela foi criada por um programa desenvolvido pela *Advanced Research Projects Agency (ARPA)* mais tarde rebatizada como DARPA.

A agência nasceu de uma iniciativa do departamento de defesa dos Estados Unidos, na época preocupado em não perder terreno na corrida tecnológica deflagrada pelos russos com o lançamento do satélite Sputinik, em 1957. Roberts, acadêmico do MIT (Instituto de Tecnologia de Massachusetts), era um dos integrantes da DARPA e um dos pais da ARPANET, que começou em 1969 conectando quatro universidades: UCLA – Universidade da Califórnia em Los Angeles, Stanford, Santa Bárbara e Utah. A separação dos militares da ARPANET só ocorreu em 1983, com a criação da Milnet.

A comunicação entre os dispositivos vem aumentando exponencialmente, porém para quando falamos comunicação entre computadores, telefones, receptores de TV, câmeras ou em qualquer outro tipo de dispositivo é necessário uma gama muito grande de componentes sejam eles via software ou hardware. Neste capítulo veremos como é feito o cabeamento estruturado, seus padrões, normas e o cabeamento horizontal e vertical.

O cabeamento estruturado surgiu como resposta ao avanço das telecomunicações com o objetivo de criar uma padronização do cabeamento instalado dentro de edifícios comerciais e residenciais independente das aplicações a serem utilizadas no mesmo.

O sistema de cabeamento estruturado proporciona ao usuário a possibilidade de utilização de um computador, um telefone, uma câmera de vídeo, um alto-falante, um sensor de temperatura, presença, etc. De maneira simples e organizada, bastando para isso "plugar" o equipamento, como no sistema elétrico, em uma tomada (outlet) e fazer a manobra do cabo correspondente àquele ponto, no "armário de telecomunicação" e ou "sala de equipamentos".

15.2 - CARACTERÍSTICAS DO CABEAMENTO ESTRUTURADO

O cabeamento estruturado proporciona as empresas, integração com os mais variados tipos de dispositivos, montando quase tudo em uma única estrutura, que se for bem organizada fornecerá redução de custo em longo prazo. Sendo assim o cabeamento é um fator muito importante em um projeto de rede que se deve ter muita atenção, pois influenciará totalmente na performance de toda a rede, assim como a confiabilidade da mesma. O sistema de cabeamento estruturado possui as seguintes características:

- Facilidade de mudanças de layout.
- Pronto atendimento às demandas de comunicação dos usuários.
- Diminuição nos custos de mão de obra e montagem de infraestrutura.

- Maior confiabilidade no sistema de cabeamento.
- Facilidade no acesso e processamento de informações.
- Integração de sistemas de controle através do cabeamento.
- Um único cabeamento para diversas aplicações.

Para que tais qualidades sejam aplicadas em um projeto de rede é necessário se entender e aplicar as estruturas do cabeamento estruturado. Só assim será possível atingir os objetivos propostos pelo projeto.

15.3 - CABEAMENTO ESTRUTURADO[19]

O cabeamento em sua estrutura está dividido em seis classes de funcionalidade, descritas logo abaixo:

1. **Área de Trabalho (*Work Área*)** - como no nome já diz, compreende a área destinada aos telefones, tomada de telecomunicações, computadores, terminais de dados.

2. **Sala de Equipamento (*Equipment Room*)** - onde se localizam os equipamentos ativos do sistema, bem como as interligações com sistemas externos, por exemplo, central telefônica, servidor de rede, central de alarme e etc. Recomenda-se que seja um ambiente especialmente reservado para este fim, com as dimensões recomendadas na norma, conforme as necessidades de cada edificação.

3. **Entrada de Telecomunicações (*Entrance Facility*)** - toda infraestrutura de instalações de entrada no edifício que faz a interface com o cabeamento externo (provedores de serviço e interligação de campus).

4. **Cabeamento Secundário (*Horizontal Cabling*)** - é o cabeamento que vai dos armários até a saída da área de trabalho.

5. **Cabeamento Primário (*Backbone Cabling*)** - cabeamento que faz a interligação entre os armários de telecomunicações, salas de equipamentos e instalações de entrada, ou seja, ligação vertical entre pisos, cabos entre sala de equipamentos e entrada do edifício entre outros.

6. **Salas de Telecomunicações (*Telecommunication Room*)** - tem a função de receber o cabeamento horizontal, abrigar o cross-connect, fazer a interconexão com o backbone e também alojar os equipamentos ativos básicos.

Estes elementos funcionais descritos acima têm como objetivo prover as especificações do projeto e direção para todas as instalações do prédio relacionadas aos sistemas de cabeamento estruturado e componentes. Essas características identificam e endereçam seis componentes proeminentes da infraestrutura do prédio: facilidade de entrada, sala(s) de equipamentos, rotas principais (de backbone[20]), armários de telecomunicações, rotas secundárias (horizontais) e áreas de trabalho.

Por essas e outras vantagens o cabeamento estruturado passou a ser bastante usado nas empresas, com isso várias empresas fornecedoras da tecnologia começaram a desenvolver seus produtos sendo que cada uma tinha o seu padrão de estruturação. Sendo assim vários problemas de integração começaram a surgir, a partir desse momento começaram a se pensar em um dos padrões.

---

19 - José Maurício Santos Pinheiro - Professor Universitário, Projetista e Gestor de Redes, membro da BICSI, Aureside, IEC.

20 - Backbone significa "espinha dorsal", e é o termo utilizado para identificar a rede principal pela qual os dados de todos os clientes da internet passam. É a espinha dorsal da internet.

15.4 - NORMAS ESTRUTURAIS

Reconhecendo a necessidade de padronizar o sistema de cabeamento estruturado diversos profissionais, fabricantes, consultores e usuários reuniram-se sob a orientação de organizações como ISO/IEC, TIA/EIA, CSA, ANSI, BICSI e outras para desenvolver normas para garantir a implementação do conceito do mesmo.

15.5 - PRINCIPAIS NORMAS:

A EIA / TIA edita os TSB (T*echnical Systems Boletins*), que fazem ajustes nas normas com revisões de 5 em 5 anos. Servem de referência para as normas dos países (ABNT)
É comum se usar ANSI / EIA / TIA. No Brasil utiliza-se à ABNT.

• ANSI / EIA / TIA 568 – Norma para cabeamento de edifícios comerciais em junho 1991 foi o primeiro documento sobre normas de cabeamento em telecomunicações.
• ANSI / EIA / TIA TSB 36 – Boletim de especificações técnicas para cabos UTP fornece informações sobre o cabo UTP que não haviam sidos contemplados na Norma 568, em agosto 1991.
• ANSI / EIA / TIA TSB 53 – Boletim de especificações técnicas para hardware de conexão em cabos STP fornece informações sobre conectores, tomadas e painéis de distribuição que conectam os cabos STP, em março 1992.
• ANSI / EIA / TIA TSB 40A – Boletim de especificações técnicas para hardware de conexão em cabos UTP especifica critérios de desempenho para hardwares que conectam os cabos UTP relacionados na TBS 36 e especificar características para os cabos de conexão dos painéis de distribuição aos equipamentos ativos, em janeiro 1994.
• ANSI / EIA / TIA 568B – Primeira revisão da norma para cabeamento em edifícios comerciais. Engloba os boletins TSB 40, 36 e 53. Inclui tomadas internas, conexões entre prédios e cabeamento em campus, em outubro 1995.
• ANSI / EIA / TIA 569A – Normas para edificação dos caminhos e espaços de telecomunicações em edifícios comerciais, já é uma revisão da Norma 569 de outubro de 1990. Padroniza o projeto de construção da infraestrutura que suportará o sistema de cabeamento, especificando ainda salas, áreas de caminhos onde os cabos e os equipamentos de telecomunicações estarão.
• ANSI / EIA / TIA 606A – Normas para administração da infraestrutura de telecomunicações em edifícios comerciais especifica os padrões de administração em maio 2002.
• ANSI / EIA / TIA TSB 67 – Especifica técnicas de medição em campo do link de transmissão de cabos UTP determina as características dos equipamentos, parâmetros mínimos e métodos de testes para cabos UTP nas várias categorias, em outubro 1995.
• ANSI / EIA / TIA 568-B3 – Componentes para cabeamento de fibra óptica:

- Cabos.
- Conectores.
- Hardware de conexão.
- Patch cords.
- Teste.
- Cabos multimodo e monomodo.

15.6 - EXERCÍCIO PROPOSTO

1 - Cite três características do cabeamento estruturado.

_____
_____
_____

16 – ELEMENTOS ATIVOS

Os elementos ativos de uma rede de computadores são utilizados para interligar essas redes, esses dispositivos funcionam em diferentes camadas da arquitetura da rede. É todo e qualquer dispositivo físico energizado em uma rede de computadores.

16.1 - ATIVOS DE REDE

Sem eles a sua rede simplesmente não terá utilidade. E você só percebe que eles existem quando há problema ou algum serviço importante sai do ar.

Quando os elementos ativos são mal configurados podemos notar alguns problemas na rede, tais como: lentidão na internet, erro ao tentar salvar arquivos na rede, aplicações que travam com frequência e até vazamento de informações.

São cinco tipos de ativos de rede: repetidores, hub, bridges, switches de camada 2 e 3, roteadores. Repetidores e hub´s operam somente na 1ª camada da arquitetura da internet, as bridges e os switches de camada 2 operam nas duas primeiras camadas, os roteadores e os switches de 3ª camada funcionam nas três primeiras camadas,

16.2 - REPETIDORES

É um dispositivo que opera somente na camada física. Os sinais transportando informação dentro de uma rede só podem viajar distâncias fixas antes que a atenuação coloque em risco a integridade dos dados. Um repetidor recebe o sinal na entrada e, antes que o sinal torne-se muito fraco ou corrompido, regenera-o ao nível onde a inteligibilidade dos dados seja mantida. O repetido transmite para saída um sinal regenerado. A maior aplicação dos repetidores é para entender o comprimento físico de uma LAN. "Um repetidor conecta seguimentos de uma mesma LAN".

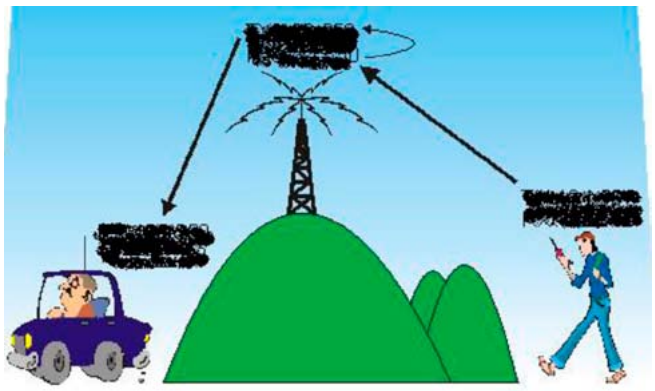


Imagem 29

16.3 - HUB

O hub é um dispositivo que tem a função de interligar os computadores de uma rede local. Sua forma de trabalho é a mais simples se comparado ao switch e ao roteador: o hub recebe dados vindos de um computador e os transmite a outras máquinas. No momento em que isso ocorre, nenhum outro computador consegue enviar sinal. Sua liberação acontece após o sinal anterior ter sido completamente distribuído.

Em um hub é possível ter várias portas, ou seja, entradas para conectar o cabo de rede de cada computador. Geralmente, há aparelhos com 8, 16, 24 e 32 portas. A quantidade varia

de acordo com o modelo e o fabricante do equipamento.

Caso o cabo de uma máquina seja desconectado ou apresente algum defeito, a rede não deixa de funcionar, pois é o hub que a "sustenta". Também é possível adicionar um outro hub ao já existente. Por exemplo, nos casos em que um hub tem oito portas e outro com igual quantidade de entradas foram adquiridos para a mesma rede.

Hubs são adequados para redes pequenas e/ou domésticas. Havendo poucos computadores é muito pouco provável que surja algum problema de desempenho.

A diferença entre os hubs e switches é que o hub apenas retransmite tudo o que recebe para todos os micros conectados a ele, como se fosse um espelho. Isso significa que apenas um micro pode transmitir dados de cada vez e que todas as placas precisam operar na mesma velocidade, que é sempre nivelada por baixo. Caso você coloque um micro com uma placa de 10 megabits na rede, a rede toda passará a trabalhar a 10 megabits.

Imagens 30 e 31

16.4 - BRIDGES21

Bridge ou ponte é o termo utilizado em informática para designar um dispositivo que liga duas ou mais redes informáticas que usam protocolos distintos ou iguais ou dois segmentos da mesma rede que usam o mesmo protocolo, por exemplo, Ethernet ou token ring. Bridges servem para interligar duas redes, como, por exemplo, ligação de uma rede de um edifício com outro. Uma bridge é um segmento livre entre rede, entre o servidor e o cliente (tunel), possibilitando a cada usuário ter sua senha independente.

Uma bridge ignora os protocolos utilizados nos dois segmentos que liga, já que opera a um nível muito baixo do modelo OSI (nível 2); somente envia dados de acordo com o endereço do pacote. Este endereço não é o endereço IP (Internet Protocol), mas o MAC (Media Access Control) que é único para cada placa de rede. Os únicos dados que são permitidos atravessar uma bridge são dados destinados a endereços válidos no outro lado da ponte. Desta forma é possível utilizar uma bridge para manter um segmento da rede livre dos dados que pertencem a outro segmento.

É frequente serem confundidos os conceitos de bridge e concentrador (ou hub); uma das diferenças, como já anunciado, é que o pacote é enviado unicamente para o destinatário, enquanto que o hub envia o pacote em broadcast.

---

21 - Bridge ou ponte é o termo utilizado em **informática** para designar um dispositivo que liga duas ou mais **redes** informáticas que usam **protocolos** distintos ou iguais ou dois segmentos da mesma rede que usam o mesmo protocolo, por exemplo, **Ethernet** ou **Token Ring**. Bridges servem para interligar duas redes, como por exemplo, ligação de uma rede de um edifício com outro. Uma bridge é um segmento livre entre rede, entre o servidor e o cliente (tunel), possibilitando a cada usuário ter sua senha independente.

16.5 - SWITCHES

Os switches por sua vez são aparelhos muito mais inteligentes. Eles fecham canais exclusivos de comunicação entre o micro que está enviando dados e o que está recebendo, permitindo que vários pares de micros troquem dados entre si ao mesmo tempo. Isso melhora bastante a velocidade em redes congestionadas, com muitos micros. Outra vantagem dos switches é que eles permitem o uso do modo full-duplex, onde é possível enviar e receber dados simultaneamente. Isso permite que os micros disponham de 100 ou 1000 megabits em cada sentido, agilizando as transmissões.

Outra importante diferença está relacionada à gestão da rede, com um switch gerenciável, podemos criar WLAN´s, deste modo à rede gerida será divida em menores segmentos.

Como se diz, "o switch aprende com a rede e depois só encaminha para endereços conhecidos", mas como se faz isto? Quando você liga um switch a uma rede, ele não conhece a rede ainda, então ele precisará aprender com a rede, então vamos ver, funciona assim: considere uma rede com 4 computadores (computador A, computador B, computador C e computador D) conectados nas portas 1, 2, 3 e 4 respectivamente, o computador A envia um quadro ao computador D (eu sou o computador A e quero enviar este quadro ao computador D), o switch ainda não sabe onde está o computador D por isso ele faz broadcast para todas as outras 3 portas (2, 3 e 4), mas ele já gravou que o computador A está na porta 1. Num outro momento, o computador C envia um quadro ao computador A, então o switch não faz mais broadcast porque ele já aprendeu que o computador A está na porta 1, então ele envia somente para esta porta, e também já aprendeu que o computador C está na porta 3, e assim sucessivamente até aprender em quais portas estão todos os computadores da rede, a partir e então ele envia somente à porta de destino específico (Unicast).

Imagens 32 e33

16.6 – ROTEADORES

Assim como um computador, um roteador ou switch não pode funcionar sem um sistema operacional. Essa é a tecnologia de software embutida em todos os roteadores e switches, sendo também o sistema operacional dos switches e roteadores. Sem um sistema operacional, o hardware não tem qualquer funcionalidade.

16.6.1 - SERVIÇOS OFERECIDOS

- Funções Básicas de roteadores e switches.
- Confiável e seguro aos recursos da rede.
- Escalabilidade.[22]

22 - Escalabilidade é uma característica desejável em todo o sistema, em uma rede ou em um processo, que indica sua habilidade de manipular uma porção crescente de trabalho de forma uniforme.

16.6.2 - COMPONENTES DOS ROTEADORES

Roteadores e computadores possuem quatro componentes comuns básicos:

- CPU.
- Barramento.
- Memória.
- Interfaces.

A imagem abaixo mostra a funcionalidade dos roteadores. Observem as rotas.

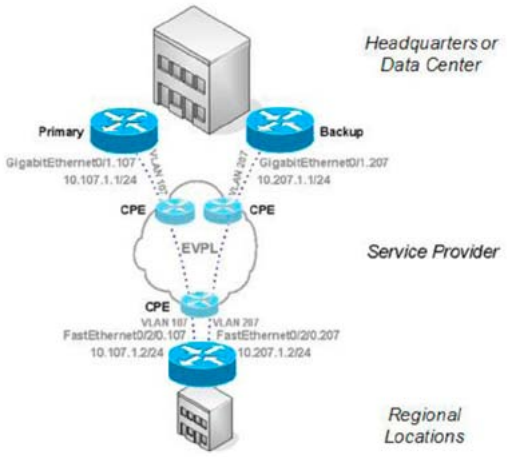


Imagem 34

16.7 – EXERCÍCIO PROPOSTO

1 - Defina Hub?

_____
_____
_____

17 – CABOS E CONECTORES

Observamos que ao longo dos anos muito se tem discutido e falado sobre as novas tecnologias envolvendo hardware e software de redes disponíveis no mercado. Não deixemos nos enganar pesando que estes produtos podem resolver todos os problemas de processamento da empresa. Infelizmente, o investimento em equipamentos envolve valores elevados, é necessário que se dê também atenção especial à estrutura de cabeamento, ou cabling, pois é composto importante para o sucesso de ambientes distribuídos. Conforme pesquisas de órgãos internacionais, o cabeamento hoje é responsável por 80% das falhas físicas de uma rede e, oito em cada dez problemas detectados referem-se a cabos mal-instalados ou em estado precário. Existem basicamente três tipos diferentes de cabos de rede:

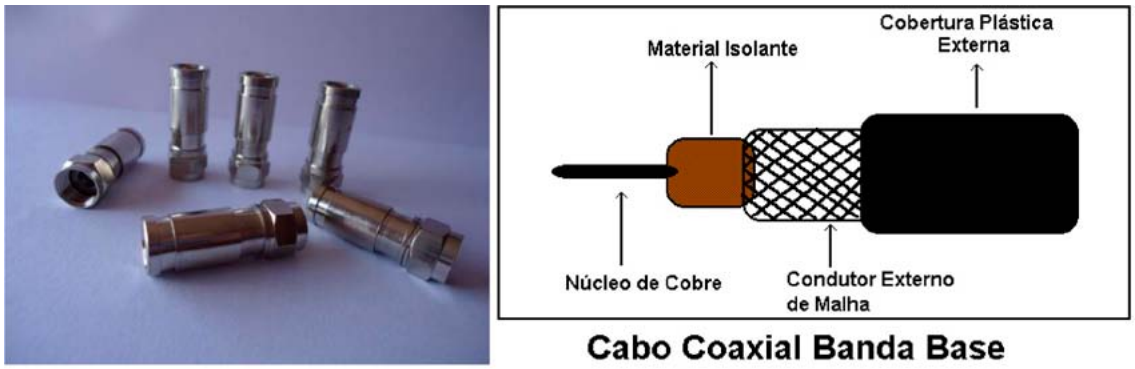
1. Os cabos de par trançado (que são, de longe, os mais comuns),
2. Os cabos de fibra óptica (usados principalmente em links de longa distância)
3. Os cabos coaxiais, ainda usados em algumas redes antigas.

Existem vários motivos para os cabos coaxiais não serem mais usados hoje em dia: eles são mais propensos a mau contato, os conectores são mais caros e os cabos são menos flexíveis que os de par trançado, o que torna mais difícil passá-los por dentro de tubulações. No entanto, o principal motivo é o fato de que eles podem ser usados apenas em redes de 10 megabits: a partir do momento em que as redes 10/100 tornaram-se populares, eles entraram definitivamente em desuso, dando lugar aos cabos de par trançado. Entre eles, os que realmente usamos no dia a dia são os cabos "cat 5" ou "cat 5e", onde o "cat" é abreviação de "categoria" e o número indica a qualidade do cabo.

17.1 - TIPOS DE CABOS

17.1.1 - CABO COAXIAL

O primeiro tipo de cabeamento que surgiu no mercado foi o cabo coaxial. Há alguns anos, esse cabo era o que havia de mais avançado, sendo que a troca de dados entre dois computadores era coisa do futuro. Existem vários tipos de cabos coaxiais, cada características específicas. Alguns são melhores para transmissão em alta frequência, outros têm atenuação mais baixa, e outros são imunes a ruídos e interferências. Os cabos coaxiais de alta qualidade não são maleáveis e são difíceis de instalar e os cabos de baixa qualidade podem ser inadequados para trafegar dados em alta velocidade e longas distâncias. Diferentemente do cabo de par trançado, o coaxial mantém uma capacidade constante e baixa, independente do seu comprimento, evitando assim vários problemas técnicos. Devido a isso, ele oferece velocidade da ordem de megabits/seg., não sendo necessária a regeneração do sinal, sem distorção ou eco, propriedade que já revela alta tecnologia. O cabo coaxial pode ser usado em ligações ponto a ponto ou multiponto. A ligação do cabo coaxial causa reflexão devido a impedância não infinita do conector. A colocação destes conectores, em ligação multiponto, deve ser controlada de forma a garantir que as reflexões não desapareçam em fase de um valor significativo. Grande parte dos sistemas de transmissão de banda base utilizam cabos de impedância com características de 50 Ohm, geralmente utilizados nas TV´s a cabo e em redes de banda larga. Isso se deve ao fato de a transmissão em banda base sofrer menos reflexões, devido às capacitâncias introduzidas nas ligações ao cabo de 50 Ohm. Os cabos coaxiais possuem uma maior imunidade a ruídos eletromagnéticos de baixa frequência e, por isso, eram o meio de transmissão mais usado em redes locais. A imagem abaixo mostra conectores de compressão para cabos coaxial.



Imagens 35 e 36

17.1.1.1 - MEIOS DE TRANSMISSÃO

• 50 são denominados de cabos banda básica: uma frequência de transmissão, ou duas se for utilizada modulação FSK.
• 75 são denominados de cabos banda larga: permite a multiplexação por divisão de frequência (FDM) de vários canais. Aplicações de TV a cabo.
A atenuação do sinal no cabo coaxial depende:
• do comprimento;
• das características elétricas;
• da frequência do sinal;
• do número de conectores existentes.

17.1.1.2 - TIPOS DE CABOS

TIPO DE CABO	IMPEDÂNCIA	DIÂMETRO	CONECTOR
Cabo fino Ethernet – RG - 58	50 ohms	3/16”	BNC
ARCNET – RG -62	93 ohms	3/16”	BNC
ou RG - 59/U	75 ohms	3/16”	Utiliza um rabicho RG-62 na extremidade com BNC.
Cabo espesso Ethernet	50 ohms	1/2”	Transceptor/MAU no cabo espesso com uma derivação do de par trançado até o cordão da rede.
de Ethernet espesso (não é coaxial, é um cabo de par blindado).		3/8”	DIX/AUI

17.1.2 - CABO DE PAR TRANÇADO

Com as mudanças no mundo da tecnologia, surgiu o cabeamento de par trançado. Esse tipo de cabo tornou-se muito usado devido à falta de flexibilidade de outros cabos e por causa da necessidade de se ter um meio físico que conseguisse uma taxa de transmissão alta e mais rápida. Os cabos de par trançado possuem dois fios entrelaçados em forma de espiral e, por isso, reduzem o ruído e mantém constantes as propriedades elétricas do meio, em todo o seu comprimento. A desvantagem deste tipo de cabo, que pode ter transmissão tanto analógica quanto digital, é sua suscetibilidade às interferências a ruídos

(eletromagnéticos e radiofrequência). Esses efeitos podem, entretanto, ser minimizados com blindagem adequada. Vale destacar que várias empresas já perceberam que, em sistemas de baixa frequência, a imunidade a ruídos é tão boa quanto a do cabo coaxial.

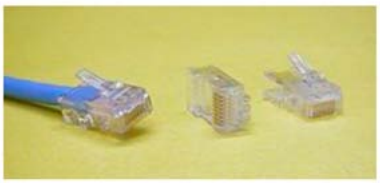
O cabo de par trançado é o meio de transmissão de menor custo por comprimento no mercado. A ligação de nós ao cabo é também extremamente simples e de baixo custo. Esse cabo se adapta muito bem às redes com topologia em estrela, onde as taxas de dados mais elevadas permitidas por ele e pela fibra óptica ultrapassam, e muito, a capacidade das chaves disponíveis com a tecnologia atual. Hoje em dia, o par trançado também está sendo usado com sucesso em conjunto com sistemas ATM para viabilizar o tráfego de dados a uma velocidade alta: 155 megabits/seg.

17.1.2.1 - TIPOS DE CABOS

TIPO DE CABO	IMPEDÂNCIA	DIÂMETRO	CONECTOR	REDE
Categoria 1	Não adequada a LAN´s.			
Categoria 2	Não adequada a LAN´s.			
Categoria 3	Até 10 Mbps	UTP 4 pares 100 ohms	568A ou 568B de 8 fios	10 Base - T
Categoria 4	Até 16 Mbps	STP 2 pares 150 ohms	STP-A	10 Base - T ou Token Ring
Categoria 5	Até 100 Mbps	UTP 4 pares 100 ohms	568A ou 568B de 8 fios.	10Base - T, 100Base - T, FDDI, ATM, Token Ring, 1000 Base T.

Observe as figuras abaixo:

Cat 5



Imagens 37, 38 e 39

17.2 - DEFINIÇÃO DAS CATEGORIAS DE CABEAMENTO

Categoria 1 - Utilizado em instalações telefônicas, porém inadequado para transmissão de dados.

Categoria 2 - Outro tipo de cabo obsoleto. Permite transmissão de dados até 2.5 megabits

e era usado nas antigas redes ARCNET.

Categoria 3 - Era o cabo de par trançado sem blindagem mais usado em redes há uma década. Pode se estender por até 100 metros e permite transmissão de dados a até 10Mbps. A principal diferença do cabo de categoria 3 para os obsoletos cabos de categoria 1 e 2 é o entrançamento dos pares de cabos. Enquanto nos cabos 1 e 2 não existe um padrão definido, os cabos de categoria 3 (assim como os de categoria 4 e 5) possuem pelo menos 24 tranças por metro e, por isso, são muito mais resistentes a ruídos externos. Cada par de cabos tem um número diferente de tranças por metro, o que atenua as interferências entre os pares de cabos. Praticamente não existe a possibilidade de dois pares de cabos terem exatamente a mesma disposição de tranças.

Categoria 4 - Cabos com uma qualidade um pouco melhor que os cabos de categoria 3. Este tipo de cabo foi muito usado em redes Token Ring de 16 megabits. Em teoria podem ser usados também em redes Ethernet de 100 megabits, mas na prática isso é incomum, simplesmente porque estes cabos não são mais fabricados.

Categoria 5 - A grande vantagem desta categoria de cabo sobre as anteriores é a taxa de transferência: eles podem ser usados tanto em redes de 100 megabits, quanto em redes de 1 gigabit.

Categoria 5e - Os cabos de categoria 5e são os mais comuns atualmente, com uma qualidade um pouco superior aos cat 5. Eles oferecem uma taxa de atenuação de sinal mais baixa, o que ajuda em cabos mais longos, perto dos 100m permitidos. Estão disponíveis tanto cabos blindados, quantos cabos sem blindagem, os mais baratos e comuns. Além destes, temos os cabos de categoria 6 e 7, que ainda estão em fase de popularização.

Categoria 6 - Utiliza cabos de quatro pares, semelhantes aos cabos de categoria 5 e 5e. Este padrão não está completamente estabelecido, mas o objetivo é usá-lo (assim como os 5e) nas redes Gigabit Ethernet. Já é possível encontrar cabos deste padrão à venda em algumas lojas.

Categoria 7 - Os cabos cat 7 também utilizam quatro pares de fios, porém usam conectores mais sofisticados e são muito mais caros. Tanto a frequência máxima suportada, quanto a atenuação de sinal são melhores do que nos cabos categoria 6. Está em desenvolvimento um padrão de 10 Gigabit Ethernet que utilizará cabos de categoria 6 e 7.

17.2.1 - VANTAGENS DO CABO UTP

1 - Não tem blindagem, portanto não necessita de aterramento.
2 - Mantém impedância constante de 100 OHMS sem terminadores.
3 - Cabo leve, fino, de baixo valor por metro (R$0,70) e de conectores baratos para 8 (oito) contatos. (R$0,90)
4 - No cabeamento estruturado para o cabo UTP, quando há mau contato ou o cabo é interrompido, apenas um micro para de funcionar, enquanto o resto da rede continua funcionando normalmente.
5 - Permite taxas de transmissão da ordem de 155 Mb/s por par.

17.3 - FIBRA ÓPTICA

Quando se fala em tecnologia de ponta, o que existe de mais moderno são os cabos de fibra óptica. A transmissão de dados por fibra óptica é realizada pelo envio de um sinal de luz codificado, dentro do domínio de frequência do infravermelho a uma velocidade de 10 a 15 MHz. O cabo óptico consiste de um filamento de sílica e de plástico, onde é feita a transmissão da luz.

As fontes de transmissão de luz podem ser diodos emissores de luz (LED) ou lasers semicondutores. O cabo óptico com transmissão de raio laser é o mais eficiente em potência

devido a sua espessura reduzida. Já os cabos com diodos emissores de luz são muito baratos, além de serem mais adaptáveis à temperatura ambiente e de terem um ciclo de vida maior que o do laser.

Apesar de serem mais caros, os cabos de fibra óptica não sofrem interferências com ruídos eletromagnéticos e com radiofrequências e permitem um total isolamento entre transmissor e receptor. Portanto, quem deseja ter uma rede segura, preservar dados de qualquer tipo de ruído e ter velocidade na transmissão de dados, os cabos de fibra óptica são a melhor opção do mercado.

O cabo de fibra óptica pode ser utilizado tanto em ligações ponto a ponto quanto em ligações multiponto. A exemplo do cabo de par trançado, a fibra óptica também está sendo muito usada em conjunto com sistemas ATM, que transmitem os dados em alta velocidade. O tipo de cabeamento mais usado em ambientes internos (LAN´s) é o de par trançado, enquanto o de fibra óptica é o mais usado em ambientes externos.

Apenas para complementar: O cabeamento de fibra óptica teria uma largura de banda típica em torno de 1ghz, o suficiente para utilizarem-se os serviços mais corriqueiros da internet (FTP, e-mail, Web, videoconferência e etc.) com muita folga, assumindo-se um comprimento máximo de 1,5 KM.

17.3.1 – SISTEMA DE TRANSMISSÃO

Um sistema de transmissão óptico tem três componentes:

- A fonte de luz.
- Luz policromático de comprimento de onda centrado em 0.8m.
- Sinal produzido por LED ou por laser semicondutor.

17.3.2 - O MEIO DE TRANSMISSÃO (FIBRA)

O detector: Fotodetectores, transforma sinais óticos em sinais elétricos, photodiodos (tempo de resposta em torno de 1hs 1Gbps).

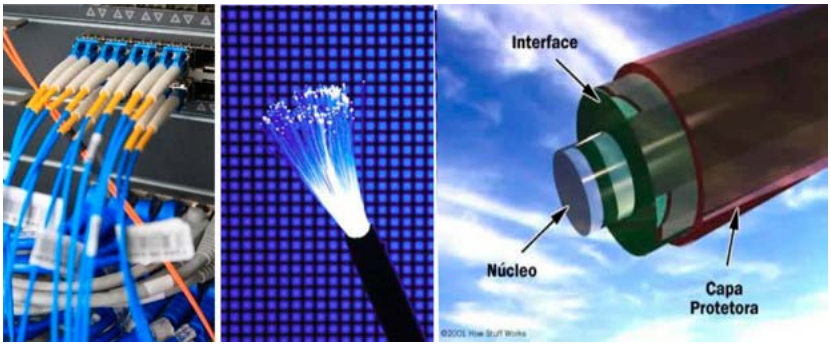
17.4 - PRINCÍPIO DE FUNCIONAMENTO

17.4.1 - TIPOS DE FIBRAS

- **Multimodo** - possui vários modos, devido ao fenômeno de espalhamento do sinal.
- **Monomodo** - devido a possuírem diâmetros de apenas alguns comprimentos de ondas, elas funcionam como guias de onda.

Fibras monomodos são mais precisas que fibras multimodos.
Fibras monomodos são mais caras que fibras multimodos.

Observe as imagens abaixo:



Imagens 40,41 e 42

17.5 - CONECTORES [23]

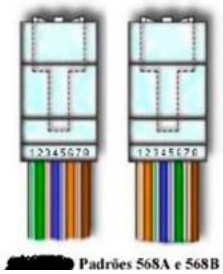
Nas redes de cabos UTP, a Norma EIA/TIA padronizou o conector RJ-45 para a conectorização de cabos UTP. São conectores que apresentam uma extrema facilidade de manuseio, tempo reduzido na conectorização e confiabilidade, sendo que estes fatores influem diretamente no custo e na qualidade de uma instalação. Os conectores estão divididos em dois tipos: macho (plug) e fêmea (jack). O conector RJ-45 macho possui um padrão único no mercado, no que diz respeito ao tamanho, formato e em sua maior parte material, pois, existem vários fabricantes deste tipo de conector, portanto todos devem obedecer a um padrão para que qualquer conector RJ-45 macho de qualquer fabricante seja compatível com qualquer conector RJ-45 fêmea de qualquer fabricante. Já o conector RJ-45 fêmea pode sofrer algumas alterações com relação à sua parte externa.

Para a conectorização do cabo UTP, a Norma EIA/TIA 568 A/B determina a pinagem e configuração. Esta norma é necessária para que haja uma padronização no mercado. Contudo, existem, no mercado, duas padronizações para a pinagem categoria 5, o padrão 568 A e 568 B, que diferem apenas nas cores de dois pares de condutores do cabo UTP.

17.6 – INSTALAÇÃO

Devem ser obedecidos os seguintes procedimentos:
1 - Decapar a capa externa do cabo cerca de 20 mm.
2 - Posicionar os pares de condutores lado a lado, com cuidado de não misturar os fios entre si. Utilizar um dos padrões de conexão: T568A ou T568B.
3 - Destorcer e posicionar os condutores segundo a tabela abaixo.

Tabela - Pinagens do Conector RJ-45 Macho	
EIA/TIA-568A	EIA/TIA-568B
1. Branco-Verde	1. Branco-Laranja
2. Verde	2. Laranja
3. Branco-Laranja	3. Branco-Verde
4. Azul	4. Azul
5. Branco-Azul	5. Branco-Azul
6. Laranja	6. Verde
7. Branco-Marrom	7. Branco-Marrom
8. Marrom	8. Marrom



Padrões 568A e 568B

4 - Cortar as pontas dos condutores expostos de forma que os condutores fiquem paralelos entre si.

5 - Inserir o cabo no conector com a trava voltada para baixo. Certificar que os condutores estão nas posições corretas e totalmente inseridos no conector nas respectivas cavidades. A capa externa do cabo UTP deve ser inserida até a entrada dos condutores nas cavidades dos contatos.

6 - Inserir o conector no alicate de "crimpar" mantendo-o devidamente posicionado e "crimpar" firmemente.

23 - Extraído de: http://www.malima.com.br/article_read.asp?id=37

OBS: O conector pode ser crimpado somente uma vez, não permitindo uma segunda tentativa. Após a crimpagem, certifique se os condutores estão bem crimpados e a capa do cabo esteja presa firmemente.

17.7 - RJ-45 FÊMEA (JACK)

- **Aplicação** - Conexões de terminações de cabos UTP de condutores sólidos (solid wire) com bitolas de 22 a 26 AWG.
- **Funcionamento** - Conexão com conectores RJ-45 macho através do contato elétrico e de travamento mecânico (trava do conector fêmea).
- **Material** - Corpo principal em termoplástico fosco classe UL V-0 com 8 contatos metálicos banhados com uma fina camada em ouro e terminal de contatos para os cabos UTP do tipo 110 IDC.

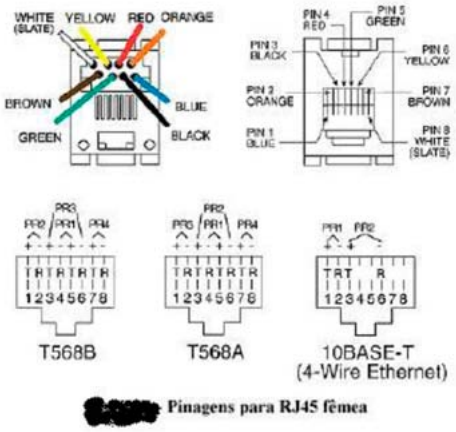


Imagem 45

17.7.1 – INSTALAÇÃO

Devem ser obedecidos os seguintes procedimentos:

1 - Preparação do cabo - Decapar a capa externa cerca de 50 mm com o cuidados de não danificar os condutores. Observar a posição final do conector na tomada ou espelho, efetuando a acomodação do cabo.

2 - Em um dos lados do conector, posicionar os dois pares dos condutores nos terminais ordenadamente segundo a correspondência de cores.

3 - Inserir os condutores com a ferramenta "110 Puch Down Tool" na posição de baixo impacto - perpendicular ao conector apoiando-o contra uma base firme e com o auxílio do suporte que acompanha o produto. Com o uso da ferramenta "110 Puch Down Tool" as sobras dos fios são automaticamente cortadas.

4 - Repetir os passos 2 e 3 com os outros 2 pares para o lado oposto do conector.

5 - Acomodar o cabo convenientemente e encaixar as travas de segurança manualmente sobre os terminais.

6 - Encaixar o conector na tomada ou espelho e identificar o ponto com os ícones de identificação.

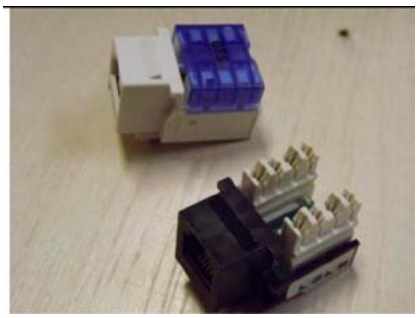
7 - Como o conector inclinado, encaixe a trava fixa na parte inferior da abertura do espelho e empurre até a trava flexível ficar perfeitamente encaixada.

8 - Após a instalação do conector RJ-45 fêmea, encaixar a tampa de proteção do conector que acompanha o produto (dust cover).

OBS: O raio de curvatura do cabo não deve ser inferior a quatro vezes o diâmetro do mesmo (21,2 mm) e evitar que o comprimento dos pares destorcidos ultrapasse 13mm.

17.8 - IMAGENS DE EQUIPAMENTOS PARA CABEAMENTO

Neste item, colocamos algumas imagens da estrutura de cabeamento para que seja fixado em sua mente de uma melhor forma.

	CONECTORES
	CONECTORES
	CABOS DE PAR TRANÇANDO (UTP) ALICATE DE CRIMPAR
	CABOS DE PAR TRANÇANDO (UTP) TEST CABLE

	TEST CABLE
	PATCH CORD
	RACK FECHADO
	RACK ABERTO

	NO BREAKS
	NO BREAKS

17.9 – EXERCÍCIO PROPOSTO

1 - O primeiro tipo de cabeamento que surgiu no mercado foi?

_____
_____
_____

18 – PROJETANDO UMA ESTRUTURA E UTILIZAÇÃO DE EQUIPAMENTOS PARA INFRAESTRUTURA DE CABEAMENTO

Neste capítulo queremos passar algumas informações sobre um projeto de infraestrutura de cabeamento e, a necessidade de conhecer equipamentos que ajudarão na elaboração de um bom projeto de redes estruturadas. Ao iniciarmos o levantamento das necessidades dos serviços que irão existir em um prédio comercial, edifício e sala, devemos ter em mente que existirão serviços que irão prover conforto, segurança e bem-estar para seus ocupantes. Quando se projeta uma estrutura de cabeamento deve-se levar em conta que estes serviços são necessários e irão existir em algum ponto da vida útil do escritório, comércio, empresa.

Devemos pensar de forma ampla, futura, crescente, pensando também no presente, é importante que o layout seja conhecido, definido, para não ter que ser constantemente reformulado, apesar de sabermos que poderá sofrer alterações e isso devemos ter ao menos uma previsão.

18.1 - LEVANTAMENTO DAS NECESSIDADES

Quando iniciarmos o projeto do sistema de cabeamento estruturado, devemos fazer um levantamento necessidades, mas, via de regra, dificilmente ocorre, então inicialmente, devemos ter em mente algumas ideias.

18.1.1 - NECESSIDADES DOS FUTUROS USUÁRIOS

1. Voz.
2. Dados.
3. Vídeo.
4. Segurança.
5. Controles ambientais.
6. Sistemas de comunicação e chamada.

18.2 - LEVANTAMENTO POR ÁREA

Área de Trabalho *(Work Area)*	Equipamento da estação: computadores, terminais de dados, telefones, faxes e outros. Cabos de ligação: são cordões de ligação, cabos adaptadores, cabos p/ PC's, impressoras e cordões de fibras ópticas. Adaptadores: baloons, adaptadores Ethernet, etc. De acordo com as normas, os adaptadores devem ser externos ao sistema de cabeamento. Tomadas para ligação dos equipamentos, para os cabos UTP, STP, fibra óptica.
Sala de Equipamento *(Equipment Room)*	Switch, roteadores, bancos de modem, centrais telefônicas
Entrada de Telecomunicações *(Entrance Facility)*	Toda infraestrutura de instalações de entrada no edifício que faz a interface com o cabeamento externo (provedores de serviço e interligação de campus).

Cabeamento Secundário *(Horizontal Cabling)*	Cabeamento que vai dos armários até a saída da área de trabalho.
Cabeamento Primário *(Backbone Cabling)*	Cabeamento que faz a interligação entre os armários de telecomunicações, salas de equipamentos e instalações de entrada, ou seja, ligação vertical entre pisos, cabos entre sala de equipamentos e entrada do edifício entre outros
Salas de Telecomunicações *(Telecommunication Room)*	Tem a função de receber o cabeamento horizontal, abrigar o cross-connect, fazer a interconexão com o backbone e também alojar os equipamentos ativos básicos.

18.3 - COMPONENTES

Segue abaixo uma descrição de componentes do cabeamento estruturado.

1 - Os componentes de conexão, tomadas, painéis de conexão, conectores, blocos e outros.
2 - Cabos de fibra óptica:

- **OFC** – cabo óptico condutivo.
- **OFCP** – cabos condutivos para dutos em forro suspenso (Plenum).
- **OFCR** – cabos condutivos para distribuição vertical (Plenum).
- **OFN** – cabo óptico não condutivo.
- **OFNP** – cabo óptico não condutivo para dutos em forro suspenso (Plenum).
- **OFNR** – cabos ópticos não condutivos para distribuição vertical (Riser).

3 - Tomadas, painéis de conexão (Patch panels), conectores (Connecting Blocks) e blocos. conectores RJ-45.
4 - *Patch panels.*
5 - *Eletrocalhas – eletrodutos – canaletas PVC.*

18.4 - PATCH PANEL

Patch panels são painéis de conexão utilizados para a manobra de interligação entre os pontos da rede e os equipamentos concentradores da rede. É constituído de um painel frontal onde estão localizados os conectores RJ-45 fêmea e de uma parte traseira onde estão localizados os conectores que são do tipo "110 IDC". Os cabos de par trançado que chegam dos pontos da rede são ligados nesses conectores e, nos conectores RJ-45 fêmea são ligados os cabos pré-conectorizados com conectores RJ-45 macho (patch cables). Os cabos denominados patch cables fazem a ligação entre o concentrador e o painel (patch panel). O patch panel tem a função de uma interface flexível, ou seja, através dele é possível alterar-se o layout lógico dos pontos da rede. Além disso, os patch panels, juntamente com as tomadas providas de conectores RJ-45 fêmea, proporcionam a rede uma grande flexibilidade em termos de deslocamento de pontos e eventuais extensões da localização de pontos de rede. Por exemplo, através dos patch panels e tomadas é possível conectar-se os cabos pré-conectorizados aos equipamentos com o comprimento necessário, isto desde que o comprimento total do lance esteja dentro do permitido pela Norma EIA/TIA. Portanto, verificamos que as tomadas e os patch panels são acessórios importantíssimos de um cabeamento estruturado. Os fabricantes normalmente dispõem de três modelos de patch panel, de 24, 48 e 96 posições.

18.5 – NO-BREAKS

Preservam momentaneamente a alimentação dos equipamentos da rede, para que estes sejam desligados sem qualquer perda de dados.

18.6 – IMPORTANTE!

- Infraestrutura da rede elétrica.
- Cabeação elétrica.
- Aterramento da rede elétrica.
- Equipamentos de proteção da rede elétrica.
- Estabilizadores de tensão
- Supressores des.
- No-breaks.

OBS: A internet é um mundo de conhecimento, e sobre esses temas do item 18.6 tem uma vasta gama de informações.

18.7 - EXERCÍCIO PROPOSTO

1 - O que faz parte da sala de equipamentos?

_____
_____
_____

19 - PROJETO DE CABEAMENTO ESTRUTURADO

Nesse tópico será passada uma estrutura para que se tenha uma ideia sobre como mostrar uma documentação sobre estrutura de cabeamento. Descrevemos abaixo os passos e procedimentos para mostrar a estrutura de cabeamento.

19.1 - OBJETIVO

Projeto de cabeamento estruturado tem o objetivo de criar um modelo de cabeamento para redes de comunicação de dados entre unidades da empresa, utilizando-se dos recursos tecnológicos disponíveis no mercado, levando em consideração, custo benefício, segurança e crescimento da empresa.

19.2 - ESCOPO

Criação do projeto de rede local (LAN), instalação de equipamentos e cabeamento estruturado, empresa de pequeno a médio porte.

19.2.1 - SUMÁRIO DO PROJETO

O projeto visa à estruturação de uma área térrea e 1º andar, disponibilizando rede e telefonia, servindo como projeto para estruturação de nova rede para o 2º andar. Projeto integrando (imagem, voz e dados).

19.3 - TECNOLOGIAS

19.3.1 - REDE LÓGICA

Para redes locais o padrão utilizado será OSI. Material utilizado entre outros cabos UTP cat5, Patch panel 24. Equipamentos: servidor, switch Cisco 24p, impressoras, central telefônica.

Os serviços disponíveis na rede: transferência de arquivo, correio eletrônico, internet/ intranet, consulta a BD, sistema ERP.

Velocidade 100 Mbps.
Utilização de eletrodutos e/ou eletrocalhas para passagem cabeamento, canaletas

19.4 - ESTAÇÕES DE TRABALHO

19.4.1 - TÉRREO

Área utilizada: 12,0 m X 25,0 m = 300 m2
Estações de trabalho: 26

Distribuição dos pontos - Rede/Telefonia.
Recepção central = 1/1
Sala de petições = 3/2
Atendimento sócio jurídico = 3/2
Atendimento jurídico = 3/2
Sala 2 = 12/6
Sala 3= 6/3
Sala 4 = 2/2

19.4.2 – 1º ANDAR

Área Útil: 12,0 m X 27,0 m =324 m2
Espaço Utilizado – 21,0 X 7,0m = 147 m2
Estações de Trabalho 3

Distribuição dos pontos – Rede/Telefonia
Recepção Juiz = 1/1
Sala do Juiz = 1/1
Arquivo = 1/1

19.5 - SALA DE EQUIPAMENTOS

A centralização dos equipamentos foi disposta na sala 4.

- *Servidor.*
- *Patch Panel.*
- Switch.
- PABX.
- Rack.
- Sala climatizada.

19.6 - CABEAMENTO

Térreo

Cabos UTP – Cat5e	21 pontos x 30m = 630m	2 cabos por ponto = 1260m

1º Andar

Cabos UTP – Cat5e	3 pontos x 30m = 90 m	2 cabos por ponto = 180m

Eletrocalhas	Eletroduto	Canaleta PVC
100 X 100mm	180m	50x20mm
140m		40 Canaletas

Todos os eletrodutos deverão ser em PVC rígido bege. Quando aparentes deverão ser fixados de forma a apresentar firmeza e boa aparência; e todos os eletrodutos devem ser antichamas.

Será sempre exigido o uso de acabamento com bucha e arruela nos quadros, caixas de passagem e qualquer outro lugar onde haja terminação dos eletrodutos.

As eletrocalhas devem obrigatoriamente ser do tipo metálico rígido, dando preferência para tratamento com zincagem a quente (pós-zincagem) ou alternativamente, a frio (galvanização eletrolítica). Todo o conjunto (eletrocalha, eletroduto e acessórios) deve ser aterrado em um único ponto. O aterramento deverá atender aos requisitos da Norma TIA/EIA 607 (*Commercial Building Grounding and Bonding Requirements for Telecommunications*).

19.7 - JUNÇÃO

- Bucha + Arruela x 31 pontos = 248 unidades.

19.7.1 - LUVAS

- 1 a cada 3 m = 10 luvas.

- Conectores RJ45.
- 93 conectores.

19.7.2 - NORMAS UTILIZADAS – REDE LÓGICA

IEEE 802.3ab - Padrão Gibabit Ethernet em cabos de par trançado.
EIA / TIA 568 - A - Padrão de cabeamento.
EIA / TIA 569 - Especificações gerais para encaminhamento de cabos (infraestrutura, canaletas, bandejas, eletrodutos e calhas).
EIA / TIA 606 - Administração da documentação.
EIA / TIA 607 - Especificação de aterramento.

19.8 - LISTA DE MATERIAIS

Obs: Os valores abaixo são fictícios, preparados para este projeto.

Descrição	Unidade	Quantidade	Valor Unit.	Valor Total
Path Panel 24 cat 5e T568/b verde	Unid.	02	490,00	980,00
Tomadas M8V(fêmea)	Unid.	31	6,0	186,00
Tomadas RJ11	Unid.	21	4,5	94,50
Caixa de tomadas para RJ11	Unid.	21	5,20	109,20
Caixa de tomadas compatíveis com M8V	Unid.	31	3,20	99,20
Conectores RJ (macho)	Unid.	93	1,50	139,50
Eletrocalhas 100x100mm	mm	140	2,50	350,00
Eletroduto	mm	180	1,80	324,00
Rack	Peça	2	410,0	820,00
Bucha + arruelas	Unid.	128	0,50	64,00
PABX	Unid.	1	1500,00	1500,00
Canaleta de PVC 50x20 mm	mm	40	2,00	80,00
Cabo UTP	mm	1440	1,10	1584,00
Parafusos para as canaletas	Uni	160	0,10	16,00
Fibra óptica	mm	70	10,00	700,00
SWITCH CISCO CATALYST WS - C2950T + 02 P FIBRA	Unid.	2	6,00	13,000
Conversor de mídia - Fibra óptica para Ethernet - sc p/ RJ45	Unid.	1	195,00	195,00

19.9 - EQUIPAMENTOS

Equipamento	Modelo	Portas	Quantidade	Valor unitário	Valor total

Servidor	Torre Processador Quad-core Memória de 4GB 667MHZ (2X1GB), Dual Ranked Suporte a Near Line SAS, SAS ou SSD2 Placa de rede, 1 Gigabit Ethernet Externa; Placa de vídeo External; Unidade de 16X SATA DVD Drive1 Monitor de 17 Mouse óptico teclado USB ABNT2 Unidade de Backup interna em fita.		1	9.000,00	9.000,00
Switch	Cisco 24 p. 10/2 100 1900	24 Ethernet + 1 Uplink	02	9.000,00	18.000,00
Impressoras	HP Laserjet 2420 dn.		04	1300,00	5.200,00

19.10 - OUTROS EQUIPAMENTOS

Equipamento	Modelo	Descrição	Quantidade	Valor total
Condicionador de ar. (para sala de servidor).	Ar -condicionado Carrier Split Piso Teto 30.000 Btus/h frio 220v.	Capacidade 30.000 Btu´s/h Unidade interna: 232x1040x625 mm; Monofásico.	1	5.000,00

19.11 - CUSTO DA OBRA

Serviços de mão de obra especializada, para garantir qualidade e eficiência ao projeto. Atendimento, garantia do serviço tempo de entrega, são itens importantes para um serviço bem feito.

Tipo/Serviço	Previsão/horas	Valor/hora	Valor Total
Empresa cabeamento	110h		
Verificação e rotulação dos pontos.	8h		
Equipe de certificação dos 31 pontos de rede.	10h		

19.12 - CUSTO TOTAL

Material	

Equipamentos	
Mao de obra	
Total	

Respostas - Exercícios Propostos

CAPÍTULO 1

1 - Qual a rede chamada de "Embrião da Internet"?

R - ARPANET.

CAPÍTULO 2

1 - Para que se estabeleça a comunicação é essencial a atuação de 5 elementos básicos. Quais são eles?

R - 1 - Emissor: 2 - Receptor; 3 - Meio de transmissão; 4 - Sinal; 5 - Linguagem.

CAPÍTULO 4

1 - Como definimos dados?

R - Dados como entidades que transportam informação.

CAPÍTULO 5

1 - Quais as camadas do modelo de referência OSI?

R – Física; Enlace de dados; Rede; Transporte; Sessão; Apresentação; Aplicação.

CAPÍTULO 6

1 - Defina redes WAN.

R - WAN (Wide Area Network) - tem o objetivo de interligar computadores distantes um do outro, ou seja, computadores localizados em cidades, estados ou mesmo países diferentes.

CAPÍTULO 7

1 - Qual comando utilizado no ambiente Windows para ver o IP da máquina?

R - Ipconfig /all.

CAPÍTULO 8

1 - O que são Hostspots?

R - São pontos de acesso Wireless que permitem ao usuário conectar-se na internet estando em locais públicos como aeroportos, shoppings, hotéis, cafeterias e outros.

CAPÍTULO 9

1 - Defina Servidor.

R - Um computador, normalmente uma estação de trabalho poderosa ou um mainframe.

CAPÍTULO 10

1 - Defina Camada Física da Rede.

R - Este é o próprio meio físico da rede.

CAPÍTULO 11

1 - Defina DNS.

R - DNS – Domain Name System – Sistema de Nomes de Domínios.

CAPÍTULO 12

1 - O que é Backdoor?

R - O Backdoor se caracteriza pelo vírus que contamina a máquina através de um programa e a deixa exposta para uma futura invasão do cracker por acesso remoto.

CAPÍTULO 13

1 - O que são Logs?

R - Logs registram informações sobre o seu funcionamento e sobre eventos por eles detectados.

CAPÍTULO 14

1 - O que é Firewall?

R - É o nome dado ao dispositivo de rede, que tem por função, regular o tráfego de rede.

CAPÍTULO 15

1 - Cite três características do cabeamento estruturado.

R - Facilidade de mudanças de layout.
Pronto atendimento às demandas de comunicação dos usuários.
Diminuição nos custos de mão de obra e montagem de infraestrutura.

CAPÍTULO 16

1 - Defina Hub?

R - O hub é um dispositivo que tem a função de interligar os computadores de uma rede local.

CAPÍTULO 17

1 - O primeiro tipo de cabeamento que surgiu no mercado foi?

R - Cabo coaxial.

CAPÍTULO 18

1 - O que faz parte da sala de equipamentos?

R - Switch, roteadores, bancos de modem, centrais telefônicas.

Referências

STALLINGS, William. Redes e Sistemas de Comunicação de dados: teoria e aplicações coorporativas. Rio de Janeiro: Elsevier, 2005.

TANENBAUM, Andrew S. Redes de Computadores. 6ª Ed. Rio de Janeiro. Elsevier, 2003.

WADLOW, Thomas A. Segurança de redes: projeto e gerenciamento de redes seguras. Rio de Janeiro: Campus: 2000.

GUIA DO HARDWARE. Cabeamento Estruturado. Disponível em: http://www.hardware.com.br/livros/redes/cabeamento-estruturado.html. Acesso em 02 jun. 2011.

DICIONÁRIO INFORMAL. Disponível em: http://www.dicionarioinformal.com.br/responsividade/. Acesso em 23 mar. 2011.

TANENBAUM, Andrew S.. Computer Networks. New Jersey: Prentice Hall, 1996.
Disponível em: http://operamundi.uol.com.br/conteudo/noticias/2456/conteudo+opera.shtml
http://pt.wikipedia.org/wiki/Comunica%C3%A7%C3%A3o_em_rede. Acesso em 23 mar. 2011.

TUTORIAL TCP/IP. Disponível em: http://www.linhadecodigo.com.br/Artigo.aspx?id=134&pag=1

WIKIPEDIA, Domain Name System. Disponível em: http://pt.wikipedia.org/wiki/Domain_Name_System. Acesso em 23 mar. 2011.

WIKIPEDIA. Cabeamento Estruturado. Disponível em: http://pt.wikipedia.org/wiki/Cabeamento_estruturado. Acesso em 02 jun. 2011.

WIKIPEDIA. Cabeamento Estruturado. Disponível em: http://pt.wikipedia.org/wiki/Cabeamento_estruturado. Acesso em 02 jun. 2011.

WIKIPEDIA. Hypertext Transfer Protocol. Disponível em: http://pt.wikipedia.org/wiki/Http. Acesso em 23 mar. 2011.

WIKIPEDIA. File Transfer Protocol. Disponível em: http://pt.wikipedia.org/wiki/File_Transfer_Protocol. Acesso em 23 mar. 2011.

WIKIPEDIA. Simple Mail Transfer Protocol. Disponível em: http://pt.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol. Acesso em 23 mar. 2011.

WIKIPEDIA. Post Office Protocol. Disponível em: http://pt.wikipedia.org/wiki/Post_Office_Protocol. Acesso em 23 mar. 2011.

Referências das Imagens

Imagem 1
http://www.google.com.br/search?tbm=isch&hl=pt

Imagem 2
http://www.google.com.br/search?tbm=isch&hl=pt

Imagem 3
http://www.google.com.br/search?tbm=isch&hl=pt

Imagem 4
http://www.google.com.br/search?tbm=isch&hl=pt

Imagem 5
http://www.google.com.br/search?tbm=isch&hl=pt

Imagem 6
http://www.google.com.br/search?tbm=isch&hl=pt

Imagem 7
http://www.google.com.br/search?tbm=isch&hl=pt

Imagem 8
http://www.google.com.br/search?tbm=isch&hl=pt

Imagem 9
http://www.google.com.br/search?tbm=isch&hl=pt

Imagem 10
http://www.google.com.br/search?tbm=isch&hl=pt

Imagem 11
http://www.google.com.br/search?tbm=isch&hl=pt

Imagem 12
http://www.google.com.br/search?tbm=isch&hl=pt

Imagem 13
http://www.google.com.br/search?tbm=isch&hl=pt

Imagem 14
http://www.google.com.br/search?tbm=isch&hl=pt

Imagem 15
http://www.google.com.br/search?tbm=isch&hl=pt

Imagem 16
http://www.google.com.br/search?tbm=isch&hl=pt

Imagem 17
http://www.google.com.br/search?tbm=isch&hl=pt

Imagem 18
http://www.google.com.br/search?tbm=isch&hl=pt

Imagem 19

http://www.google.com.br/search?tbm=isch&hl=pt

Imagem 20
http://www.google.com.br/search?tbm=isch&hl=pt

Imagem 21
http://www.google.com.br/search?tbm=isch&hl=pt

Imagem 22
http://www.google.com.br/search?tbm=isch&hl=pt

Imagem 23
http://www.google.com.br/search?tbm=isch&hl=pt

Imagem 24
http://www.google.com.br/search?tbm=isch&hl=pt

Imagem 25
http://www.google.com.br/search?tbm=isch&hl=pt

Imagem 26
http://www.google.com.br/search?tbm=isch&hl=pt

Imagem 27
http://www.google.com.br/search?tbm=isch&hl=pt

Imagem 28
http://www.google.com.br/search?tbm=isch&hl=pt

Imagem 29
http://www.google.com.br/search?tbm=isch&hl=pt

Imagem 30
http://www.google.com.br/search?tbm=isch&hl=pt

Imagem 31
http://www.google.com.br/search?tbm=isch&hl=pt

Imagem 32
http://www.google.com.br/search?tbm=isch&hl=pt

Imagem 33
http://www.google.com.br/search?tbm=isch&hl=pt

Imagem 34
http://www.google.com.br/search?tbm=isch&hl=pt

Imagem 35
http://www.google.com.br/search?tbm=isch&hl=pt

Imagem 36
http://www.google.com.br/search?tbm=isch&hl=pt

Imagem 37
http://www.google.com.br/search?tbm=isch&hl=pt

Imagem 38
http://www.google.com.br/search?tbm=isch&hl=pt

Imagem 39
http://www.google.com.br/search?tbm=isch&hl=pt

Imagem 40
http://www.google.com.br/search?tbm=isch&hl=pt

Imagem 41
http://www.google.com.br/search?tbm=isch&hl=pt

Imagem 42
http://www.google.com.br/search?tbm=isch&hl=pt

Imagem 43
http://www.google.com.br/search?tbm=isch&hl=pt

Imagem 44
http://www.google.com.br/search?tbm=isch&hl=pt

Imagem 45
http://www.google.com.br/search?tbm=isch&hl=pt

alfamacursos.com.br